Prestige 623ME-T

ADSL Modem Combo for Internet Access

User's Guide

Version 3.40

February 2004

ZyXEL

Unleash Networking Power

Copyright

Copyright © 2003 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

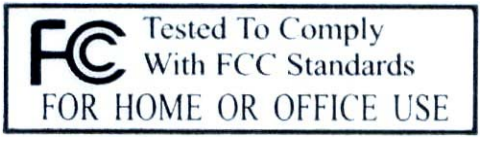
1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Certifications

1. Go to www.zyxel.com.
2. Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.



ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Safety Warnings

1. To reduce the risk of fire, use only No. 26 AWG or larger telephone wire.

2. Do not use this product near water, for example, in a wet basement or near a swimming pool.

3. Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightening.

Customer Support

Please have the following information ready when you contact customer support.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD / LOCATION	E-MAIL SUPPORT/SALES	TELEPHONE/FAX	WEB SITE/ FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu 300, Taiwan.
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-800-255-4101 +1-714-632-0858	www.us.zyxel.com ftp.us.zyxel.com	ZyXEL Communications Inc., 1130 N. Miller St. Anaheim, CA 92806, U.S.A.
SCANDINAVIA	support@zyxel.dk sales@zyxel.dk	+45-3955-0700 +45-3955-0707	www.zyxel.dk ftp.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark.
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen, Germany

Table of Contents

Copyright ..... **iii**
Federal Communications Commission (FCC) Interference Statement ..... **v**
ZyXEL Limited Warranty ..... **vii**
Customer Support ..... **ix**
List of Figures ..... **xvii**
List of Tables ..... **xxi**
List of Charts ..... **xxiii**
Preface ..... **xxv**
Introduction to DSL ..... **xxvii**
Chapter 1 Getting To Know Your Prestige **1-1**
1.1 Introducing the Prestige 1-1
1.2 Features of the Prestige 1-1
1.3 Applications for the Prestige 1-3
1.3.1 Internet Access 1-3
1.3.2 LAN to LAN Application 1-4
Chapter 2 Introducing the Web Configurator **2-1**
2.1 Web Configurator Overview 2-1
2.2 Accessing the Prestige Web Configurator 2-1
2.3 Navigating the Prestige Web Configurator 2-2
2.4 Configuring Password 2-3
2.5 Resetting the Prestige 2-4
2.5.1 Using The Reset Button 2-4
Chapter 3 Wizard Setup **3-1**
3.1 Wizard Setup Introduction 3-1
3.2 Encapsulation 3-1
3.2.1 PPPoE Encapsulation 3-1
3.2.2 RFC 1483 3-2
3.3 Multiplexing 3-2
3.3.1 VC-based Multiplexing 3-2
3.3.2 LLC-based Multiplexing 3-2
3.4 VPI and VCI 3-2
3.5 Wizard Setup Configuration: First Screen 3-2
3.6 IP Address and Subnet Mask 3-3
3.7 IP Address Assignment 3-4
3.7.1 IP Assignment with PPPoE Encapsulation 3-4
3.7.2 IP Assignment with RFC 1483 Encapsulation 3-4
3.7.3 Private IP Addresses 3-4
3.8 NAT 3-5
3.9 Wizard Setup Configuration: Second Screen 3-5

3.9.1 RFC 1483 3-5
3.9.2 PPPoE 3-6
3.10 DHCP Setup 3-7
3.10.1 IP Pool Setup 3-8
3.11 Test Your Internet Connection 3-8
Chapter 4 LAN Setup 4-1
4.1 LAN Overview 4-1
4.1.1 LANs, WANs and the Prestige 4-1
4.2 DNS Server Address 4-1
4.3 DNS Server Address Assignment 4-2
4.4 LAN TCP/IP 4-2
4.4.1 Factory LAN Defaults 4-2
4.4.2 IP Address and Subnet Mask 4-3
4.4.3 RIP Setup 4-3
4.4.4 Multicast 4-3
4.5 Configuring LAN 4-4
Chapter 5 Network Address Translation (NAT) 5-1
5.1 NAT Overview 5-1
5.2 Single User Account Server (SUA Server) 5-1
5.2.1 Advantages of SUA 5-2
5.2.2 Configuring Inside Servers 5-2
5.3 Selecting the NAT Mode 5-4
5.4 Configuring SUA Server 5-4
Chapter 6 Dynamic DNS Setup 6-1
6.1 Dynamic DNS 6-1
6.1.1 DYNDNS Wildcard 6-1
6.2 Configuring Dynamic DNS 6-1
Chapter 7 Remote Management Configuration 7-1
7.1 Remote Management Overview 7-1
7.1.1 Remote Management Limitations 7-1
7.1.2 Remote Management and NAT 7-2
7.1.3 System Timeout 7-2
7.2 Telnet 7-2
7.3 FTP 7-2
7.4 Web 7-3
7.5 Configuring Remote Management 7-3
Chapter 8 Universal Plug-and-Play (UPnP) 8-1
8.1 Universal Plug and Play Overview 8-1
8.1.1 How do I know if I'm using UPnP? 8-1
8.1.2 NAT Traversal 8-1
8.1.3 Cautions with UPnP 8-1

8.2 UPnP and ZyXEL 8-2
8.2.1 Configuring UPnP 8-2
8.3 Installing UPnP in Windows Example 8-3
8.3.1 Installing UPnP in Windows Me 8-3
8.3.2 Installing UPnP in Windows XP 8-4
8.4 Using UPnP in Windows XP Example 8-5
8.4.1 Auto-discover Your UPnP-enabled Network Device 8-5
8.4.2 Web Configurator Easy Access 8-7
Chapter 9 Maintenance 9-1
9.1 Maintenance Overview 9-1
9.2 System Status Screen 9-1
9.2.1 System Statistics 9-4
9.3 DHCP Table Screen 9-6
9.4 Diagnostic Screens 9-6
9.4.1 Diagnostic General Screen 9-7
9.4.2 Diagnostic DSL Line Screen 9-9
9.5 Firmware Screen 9-10
Chapter 10 Introducing the SMT 10-1
10.1 SMT Introduction 10-1
10.1.1 Procedure for SMT Configuration via Telnet 10-1
10.1.2 Prestige SMT Menu Overview 10-1
10.2 Navigating the SMT Interface 10-3
10.2.1 System Management Terminal Interface Summary 10-4
10.3 Changing the System Password 10-5
Chapter 11 General Setup 11-1
11.1 General Setup 11-1
11.2 Configuring Menu 1 11-1
11.2.1 Configuring Dynamic DNS 11-3
Chapter 12 LAN Setup 12-1
12.1 LAN Setup 12-1
12.1.1 LAN Port Filter Setup 12-1
12.2 Protocol Dependent Ethernet Setup 12-2
12.3 TCP/IP Ethernet Setup and DHCP 12-2
Chapter 13 Internet Access 13-1
13.1 Internet Access Overview 13-1
13.2 IP Policies 13-1
13.3 Route IP Setup 13-1
13.4 Internet Access Configuration 13-2
Chapter 14 Remote Node Configuration 14-1
14.1 Remote Node Setup Overview 14-1
14.2 Remote Node Setup 14-1

14.2.1 Remote Node Profile 14-1
14.2.2 Encapsulation and Multiplexing Scenarios 14-2
14.2.3 Outgoing Authentication Protocol 14-5
14.3 Metric 14-5
14.4 Remote Node Network Layer Options 14-6
14.4.1 My WAN Addr Sample IP Addresses 14-8
14.5 Remote Node Filter 14-9
14.5.1 Web Configurator Internet Security Filter Rules 14-10
14.5.2 Web Configurator Filter Sets 14-10
14.6 Editing ATM Layer Options 14-12
14.6.1 VC-based Multiplexing (non-PPP Encapsulation) 14-12
14.6.2 LLC-based Multiplexing or PPP Encapsulation 14-12
Chapter 15 Static Route Setup 15-1
15.1 IP Static Route Overview 15-1
15.2 Configuring an IP static route 15-2
Chapter 16 Bridging Setup 16-1
16.1 Bridging Overview 16-1
16.2 Bridge Ethernet Setup 16-1
16.2.1 Remote Node Bridging Setup 16-1
16.2.2 Bridge Static Route Setup 16-3
Chapter 17 Network Address Translation (NAT) 17-1
17.1 NAT Overview 17-1
17.2 Applying NAT 17-1
17.3 NAT Server Setup 17-3
17.4 General NAT Examples 17-3
17.4.1 Example 1: Internet Access 17-3
17.4.2 How to configure NAT 17-4
17.4.3 Example 2: Configuring an Inside Server 17-5
17.4.4 How to configure an Inside Server 17-5
Chapter 18 Filter Configuration 18-1
18.1 About Filtering 18-1
18.2 Configuring a Filter Set 18-4
18.2.1 Filter Rules Summary Menus 18-6
18.3 Configuring a Filter Rule 18-7
18.3.1 TCP/IP Filter Rule 18-7
18.3.2 Generic Filter Rule 18-12
18.4 Filter Types and NAT 18-14
18.5 Example Filter 18-14
18.6 Applying Filters and Factory Defaults 18-17
18.6.1 Ethernet Traffic 18-18
18.6.2 Remote Node Filters 18-18

Chapter 19 SNMP Configuration 19-1
19.1 SNMP Overview 19-1
19.2 Supported MIBs 19-2
19.3 SNMP Configuration 19-2
19.4 SNMP Traps 19-4
Chapter 20 System Information and Diagnosis 20-1
20.1 System Maintenance Overview 20-1
20.2 System Status 20-1
20.3 System Information 20-3
20.3.1 System Information 20-3
20.3.2 Console Port Speed 20-5
20.4 Log and Trace 20-5
20.4.1 Viewing Error Log 20-5
20.4.2 Syslog and Accounting 20-6
20.5 Diagnostic 20-8
Chapter 21 Firmware and Configuration File Maintenance 21-1
21.1 Filename Conventions 21-1
21.2 Backup Configuration 21-2
21.2.1 Backup Configuration 21-3
21.2.2 Using the FTP Command from the Command Line 21-3
21.2.3 Example of FTP Commands from the Command Line 21-3
21.2.4 GUI-based FTP Clients 21-4
21.2.5 TFTP and FTP over WAN Will Not Work When 21-4
21.2.6 Backup Configuration Using TFTP 21-5
21.2.7 TFTP Command Example 21-5
21.2.8 GUI-based TFTP Clients 21-5
21.3 Restore Configuration 21-6
21.3.1 Restore Using FTP 21-7
21.3.2 Restore Using FTP Session Example 21-8
21.4 Uploading Firmware and Configuration Files 21-8
21.4.1 Firmware File Upload 21-8
21.4.2 Configuration File Upload 21-9
21.4.3 FTP File Upload Command from the DOS Prompt Example 21-9
21.4.4 FTP Session Example of Firmware File Upload 21-10
21.4.5 TFTP File Upload 21-10
21.4.6 TFTP Upload Command Example 21-11
Chapter 22 System Maintenance 22-1
22.1 Command Interpreter Mode Overview 22-1
22.2 Call Control Support 22-2
22.2.1 Budget Management 22-2
22.3 Time and Date Setting 22-3

22.3.1 Resetting the Time 22-5
Chapter 23 Remote Management 23-1
23.1 Remote Management Overview 23-1
23.2 Configuring Remote Management 23-1
23.2.1 Remote Management Setup 23-1
23.2.2 Remote Management Limitations 23-2
23.3 Remote Management and NAT 23-3
23.4 System Timeout 23-3
Chapter 24 IP Policy Routing 24-1
24.1 IP Policy Routing Overview 24-1
24.2 Benefits of IP Policy Routing 24-1
24.3 Routing Policy 24-1
24.4 IP Routing Policy Setup 24-2
24.5 Applying an IP Policy 24-5
24.5.1 Ethernet IP Policies 24-5
24.6 IP Policy Routing Example 24-7
Chapter 25 Call Scheduling 25-1
25.1 Call Scheduling Overview 25-1
Appendix A Troubleshooting A-1
A.1 Using LEDs to Diagnose Problems A-1
A.1.1 Power LED A-1
A.1.2 LAN LED A-1
A.1.3 DSL LED A-2
A.2 Telnet A-2
A.3 Web Configurator A-3
A.4 Login Username and Password A-3
A.5 LAN Interface A-4
A.6 WAN Interface A-4
A.7 Internet Access A-5
A.8 Remote Node Connection A-6
Appendix B IP Subnetting B-1
Appendix C PPPoE C-1
Appendix D Setting up Your Computer's IP Address D-1
Appendix E Virtual Circuit Topology E-1
Appendix F Splitters and Microfilters F-1
Appendix G Power Adaptor Specifications G-1
Appendix H Index H-1

List of Figures

Figure 1-1 Internet Access Application 1-3
Figure 1-2 LAN-to-LAN Application 1-4
Figure 2-1 Password Screen 2-1
Figure 2-2 Web Configurator SITE MAP Screen 2-2
Figure 2-3 Password 2-3
Figure 3-1 Wizard Screen 1 3-3
Figure 3-2 Internet Connection with RFC 1483 3-5
Figure 3-3 Internet Connection with PPPoE 3-6
Figure 4 Setup Complete 3-8
Figure 4-1 LAN and WAN IP Addresses 4-1
Figure 4-2 LAN 4-4
Figure 5-1 Single User Account Topology 5-1
Figure 5-2 Multiple Servers Behind NAT Example 5-3
Figure 5-3 NAT Mode 5-4
Figure 5-4 Edit SUA/NAT Server Set 5-5
Figure 6-1 DDNS 6-2
Figure 7-1 Telnet Configuration on a TCP/IP Network 7-2
Figure 7-2 Remote Management 7-3
Figure 8-1 Configuring UPnP 8-2
Figure 9-1 System Status 9-2
Figure 9-2 System Status: Show Statistics 9-4
Figure 9-3 DHCP Table 9-6
Figure 9-4 Diagnostic 9-7
Figure 9-5 Diagnostic General 9-8
Figure 9-6 Diagnostic DSL Line 9-9
Figure 9-7 Firmware Upgrade 9-11
Figure 9-8 Network Temporarily Disconnected 9-12
Figure 9-9 Error Message 9-12
Figure 10-1 Login Screen 10-1
Figure 10-2 Prestige 623ME-T SMT Menu Overview 10-2
Figure 10-3 SMT Main Menu 10-4
Figure 10-4 Menu 23 System Password 10-5
Figure 11-1 Menu 1 General Setup 11-2
Figure 11-2 Menu 1.1 Configure Dynamic DNS 11-3
Figure 12-1 Menu 3 Ethernet Setup 12-1
Figure 12-2 Menu 3.1 LAN Port Filter Setup 12-1
Figure 12-3 Menu 3.2 TCP/IP and DHCP Ethernet Setup 12-2
Figure 13-1 Menu 1 General Setup 13-1
Figure 13-2 Menu 4 Internet Access Setup 13-2

Figure 14-1 Menu 11 Remote Node Setup 14-2
Figure 14-2 Menu 11.1 Remote Node Profile 14-3
Figure 14-3 Menu 11.3 Remote Node Network Layer Options 14-6
Figure 14-4 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection 14-8
Figure 14-5 Menu 11.5 Remote Node Filter (RFC 1483 Encapsulation) 14-9
Figure 14-6 Menu 11.5 Remote Node Filter (PPPoE Encapsulation) 14-9
Figure 14-7 Internet Security 14-10
Figure 14-8 Menu 21- Filer Set Configuration 14-11
Figure 14-9 Menu 21.11- WebSet 11 14-11
Figure 14-10 Menu 21.12- WebSet 12 14-11
Figure 14-11 Menu 11.6 for VC-based Multiplexing 14-12
Figure 14-12 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation 14-13
Figure 15-1 Sample Static Routing Topology 15-1
Figure 15-2 Menu 12 Static Route Setup 15-2
Figure 15-3 Menu 12.1 IP Static Route Setup 15-2
Figure 15-4 Menu12.1.1 Edit IP Static Route 15-3
Figure 16-1 Menu 11.1 Remote Node Profile 16-2
Figure 16-2 Menu 11.3 Remote Node Network Layer Options 16-2
Figure 16-3 Menu 12.3.1 Edit Bridge Static Route 16-3
Figure 17-1 Menu 4 Applying NAT for Internet Access 17-1
Figure 17-2 Menu 11.3 Applying NAT to the Remote Node 17-2
Figure 17-3 Menu 15.2.1 NAT Server Setup 17-3
Figure 17-4 Configuring NAT 17-4
Figure 17-5 Configuring NAT SMT Menus 17-4
Figure 17-6 Configuring an Inside Server 17-5
Figure 17-7 Menu 15.2.1 Specifying an Inside Server 17-5
Figure 18-1 Outgoing Packet Filtering Process 18-2
Figure 18-2 Filter Rule Process 18-3
Figure 18-3 Menu 21 Filter Set Configuration 18-4
Figure 18-4 NetBIOS_WAN Filter Rules Summary 18-5
Figure 18-5 NetBIOS_LAN Filter Rules Summary 18-5
Figure 18-6 PPPoE Filter Rules Summary 18-5
Figure 18-7 Menu 21.x.1 TCP/IP Filter Rule 18-8
Figure 18-8 Executing an IP Filter 18-11
Figure 18-9 Menu 21.6.1 Generic Filter Rule 18-12
Figure 18-10 Protocol and Device Filter Sets 18-14
Figure 18-11 Sample Telnet Filter 18-15
Figure 18-12 Menu 21.3.1 Sample Filter 18-16
Figure 18-13 Menu 21.3 Sample Filter Rules Summary 18-17
Figure 18-14 Filtering Ethernet Traffic 18-18
Figure 18-15 Filtering Remote Node Traffic 18-19

Figure 19-1 SNMP Management Model 19-1
Figure 19-2 Menu 22 SNMP Configuration 19-3
Figure 20-1 Menu 24 System Maintenance 20-1
Figure 20-2 Menu 24.1 System Maintenance : Status 20-2
Figure 20-3 Menu 24.2 System Information and Console Port Speed 20-3
Figure 20-4 Menu 24.2.1 System Maintenance : Information 20-4
Figure 20-5 Menu 24.2.2 System Maintenance : Change Console Port Speed 20-5
Figure 20-6 Menu 24.3 System Maintenance : Log and Trace 20-5
Figure 20-7 Sample Error and Information Messages 20-6
Figure 20-8 Menu 24.3.2 System Maintenance : UNIX Syslog 20-6
Figure 20-9 Menu 24.4 System Maintenance : Diagnostic 20-9
Figure 21-1 Telnet in Menu 24.5 21-3
Figure 21-2 FTP Session Example 21-4
Figure 21-3 Telnet into Menu 24.6 21-7
Figure 21-4 Restore Using FTP Session Example 21-8
Figure 21-5 Telnet Into Menu 24.7.1 Upload System Firmware 21-9
Figure 21-6 Telnet Into Menu 24.7.2 System Maintenance 21-9
Figure 21-7 FTP Session Example of Firmware File Upload 21-10
Figure 22-1 Command Mode in Menu 24 22-1
Figure 22-2 Valid Commands 22-1
Figure 22-3 Menu 24.9 System Maintenance : Call Control 22-2
Figure 22-4 Menu 24.9.1 Budget Management 22-2
Figure 22-5 Menu 24 System Maintenance 22-4
Figure 22-6 Menu 24.10 System Maintenance: Time and Date Setting 22-4
Figure 23-1 Menu 24.11 Remote Management Control 23-2
Figure 24-1 Menu 25 IP Routing Policy Setup 24-2
Figure 24-2 Menu 25.1 IP Routing Policy Setup 24-3
Figure 24-3 Menu 25.1.1 IP Routing Policy 24-4
Figure 24-4 Menu 3.2 TCP/IP and DHCP Ethernet Setup 24-6
Figure 24-5 Menu 11.3 Remote Node Network Layer Options 24-6
Figure 24-6 Example of IP Policy Routing 24-7
Figure 24-7 IP Routing Policy Example 24-8
Figure 24-8 IP Routing Policy Example 24-9
Figure 24-9 Applying IP Policies Example 24-9
Figure 25-1 Menu 26 Schedule Setup 25-1
Figure 25-2 Menu 26.1 Schedule Set Setup 25-2
Figure 25-3 Applying Schedule Set(s) to a Remote Node (PPPoE) 25-4

List of Tables

Table 2-1 Password 2-3
Table 3-1 Wizard Screen 1 3-3
Table 3-2 Internet Connection with RFC 1483 3-6
Table 3-3 Internet Connection with PPPoE 3-7
Table 4-1 LAN 4-4
Table 5-1 NAT Mode 5-3
Table 5-2 NAT Mode 5-4
Table 5-3 Edit SUA/NAT Server Set 5-6
Table 6-1 DDNS 6-2
Table 7-1 Remote Management 7-3
Table 8-1 Configuring UPnP 8-2
Table 9-1 System Status 9-2
Table 9-2 System Status: Show Statistics 9-4
Table 9-3 DHCP Table 9-6
Table 9-4 Diagnostic General 9-8
Table 9-5 Diagnostic DSL Line 9-10
Table 9-6 Firmware Upgrade 9-11
Table 10-1 Main Menu Commands 10-3
Table 10-2 Main Menu Summary 10-4
Table 11-1 Menu 1 General Setup 11-2
Table 11-2 Menu 1.1 Configure Dynamic DNS 11-3
Table 12-1 DHCP Ethernet Setup Menu Fields 12-3
Table 12-2 TCP/IP Ethernet Setup Menu Fields 12-3
Table 13-1 Menu 4 Internet Access Setup 13-2
Table 14-1 Menu 11.1 Remote Node Profile 14-3
Table 14-2 Menu 11.3 Remote Node Network Layer Options 14-7
Table 15-1 Menu12.1.1 Edit IP Static Route 15-3
Table 16-1 Menu 11.3 Remote Node Network Layer Options : Bridge Fields 16-3
Table 16-2 Menu 12.3.1 Edit Bridge Static Route 16-3
Table 18-1 Abbreviations Used in the Filter Rules Summary Menu 18-6
Table 18-2 Rule Abbreviations Used 18-6
Table 18-3 Menu 21.x.1 TCP/IP Filter Rule 18-8
Table 18-4 Menu 21.6.1 Generic Filter Rule 18-12
Table 18-5 Filter Sets Table 18-18
Table 19-1 Menu 22 SNMP Configuration 19-3
Table 19-2 SNMP Traps 19-4
Table 19-3 Ports and Interface Types 19-4
Table 20-1 Menu 24.1 System Maintenance : Status 20-2
Table 20-2 Menu 24.2.1 System Maintenance : Information 20-4

Table 20-3 Menu 24.3.2 System Maintenance : UNIX Syslog 20-6
Table 20-4 Menu 24.4 System Maintenance Menu : Diagnostic 20-9
Table 21-1 Filename Conventions 21-2
Table 21-2 General Commands for GUI-based FTP Clients 21-4
Table 21-3 General Commands for GUI-based TFTP Clients 21-6
Table 22-1 Menu 24.9.1 Budget Management 22-3
Table 22-2 Menu 24.10 System Maintenance: Time and Date Setting 22-5
Table 23-1 Menu 24.11 Remote Management Control 23-2
Table 24-1 Menu 25.1 IP Routing Policy Setup 24-3
Table 24-2 Menu 25.1.1 IP Routing Policy 24-4
Table 25-1 Menu 26.1 Schedule Set Setup 25-2

List of Charts

Chart A-1 Troubleshooting Power LED A-1
Chart A-2 Troubleshooting LAN LED A-1
Chart A-3 Troubleshooting DSL LED A-2
Chart A-4 Troubleshooting Telnet A-2
Chart A-5 Troubleshooting Web Configurator A-3
Chart A-6 Troubleshooting Internet Browser Display A-3
Chart A-7 Troubleshooting Login Username and Password A-3
Chart A-8 Troubleshooting LAN Interface A-4
Chart A-9 Troubleshooting ADSL Connection A-4
Chart A-10 Troubleshooting WAN Interface A-5
Chart A-11 Troubleshooting Internet Access A-5
Chart A-12 Troubleshooting Internet Connection A-5
Chart A-13 Troubleshooting Connecting to a Remote Node or ISP A-6
Chart B-1 Classes of IP Addresses B-1
Chart B-2 Allowed IP Address Range By Class B-2
Chart B-3 "Natural" Masks B-2
Chart B-4 Alternative Subnet Mask Notation B-3
Chart B-5 Subnet 1 ..... B-4
Chart B-6 Subnet 2 ..... B-4
Chart B-7 Subnet 1 ..... B-5
Chart B-8 Subnet 2 ..... B-5
Chart B-9 Subnet 3 ..... B-5
Chart B-10 Subnet 4 ..... B-6
Chart B-11 Eight Subnets B-6
Chart B-12 Class C Subnet Planning B-7
Chart B-13 Class B Subnet Planning B-7

Preface

Congratulations on your purchase from the Prestige 623ME-T ADSL Modem Combo for Internet Access.

Your Prestige is easy to install and configure. Use the web configurator, System Management Terminal (SMT) or command interpreter interface to configure your Prestige. Not all features can be configured through all interfaces.

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

About This User's Guide

This manual is designed to guide you through the configuration of your Prestige for its various applications. The web configurator parts of this guide contain background information on features configurable by web configurator. The SMT parts of this guide contain background information solely on features not configurable by web configurator.

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains connection information and instructions on getting started.

- Web Configurator Online Help
  Embedded web help for descriptions of individual screens and supplementary information.

- ZyXEL Glossary and Web Site
  Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

Syntax Conventions

- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.

- Mouse action sequences are denoted using a comma. For example, "click the Apple icon, **Control Panels** and then **Modem**" means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity's sake, we will use "e.g.," as shorthand for "for instance", and "i.e.," for "that is" or "in other words" throughout this manual.
- The Prestige 623ME-T may be referred to as the Prestige in this user's guide.

The following section offers some background information on DSL. Skip to *Chapter 1* if you wish to begin working with your router right away.

User Guide Feedback

Help us help you. E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

Graphics Icons Key

Prestige	Computer	Notebook computer
Server	Modem	Firewall
Telephone	Switch	Router
DSLAM		

Introduction to DSL

DSL (Digital Subscriber Line) technology enhances the data capacity of the existing twisted-pair wire that runs between the local telephone company switching offices and most homes and offices. While the wire itself can handle higher frequencies, the telephone switching equipment is designed to cut off signals above 4,000 Hz to filter noise off the voice line, but now everybody is searching for ways to get more bandwidth to improve access to the Web - hence DSL technologies.

There are actually seven types of DSL service, ranging in speeds from 16 Kbits/sec to 52 Mbits/sec. The services are either symmetrical (traffic flows at the same speed in both directions), or asymmetrical (the downstream capacity is higher than the upstream capacity). Asymmetrical services (ADSL) are suitable for Internet users because more information is usually downloaded than uploaded. For example, a simple button click in a web browser can start an extended download that includes graphics and text.

As data rates increase, the carrying distance decreases. That means that users who are beyond a certain distance from the telephone company's central office may not be able to obtain the higher speeds.

A DSL connection is a point-to-point dedicated circuit, meaning that the link is always up and there is no dialing required.

Introduction to ADSL

It is an asymmetrical technology, meaning that the downstream data rate is much higher than the upstream data rate. As mentioned, this works well for a typical Internet session in which more information is downloaded, for example, from Web servers, than is uploaded. ADSL operates in a frequency range that is above the frequency range of voice services, so the two systems can operate over the same cable.

Part I:

Getting Started

This part is structured as a step-by-step guide to help you access your Prestige. It covers key features and applications, accessing the web configurator and configuring the wizard screens for initial setup.

Chapter 1
Getting To Know Your Prestige

This chapter describes the key features and applications of your Prestige.

1.1 Introducing the Prestige

Your Prestige integrates a high-speed 10/100Mbps auto-negotiating LAN interface and a high-speed DSL port into a single package. The Prestige is ideal for high-speed Internet browsing and making LAN-to-LAN connections to remote networks. Provided with both USB and Ethernet ports, computers can share local resources (such as printers and files) and access to the Internet – simultaneously.

The web browser-based Graphical User Interface provides easy management.

1.2 Features of the Prestige

Your Prestige is packed with a number of features that give it the flexibility to provide a complete networking solution for almost any user.

Ease of Installation

Your Prestige is designed for quick, intuitive and easy installation. Physically, its compact size and lightness make it easy to position anywhere in your busy office.

USB Port

The USB port is useful if you have an USB-enabled computer that does not have a network interface card for attaching to your Ethernet network. Refer to *Quick Start Guide* for USB driver installation procedure in Windows 98 SE/Me/2000/XP.

High Speed Internet Access

The Prestige supports downstream transmission rates of up to 8Mbps and upstream transmission rates of 800 Kbps.

10/100Mbps Auto-negotiating Fast Ethernet LAN Interface

This auto-negotiation feature allows the Prestige to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

Protocols Supported

- TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.
- PPP (Point-to-Point Protocol) link layer protocol.
- Transparent bridging for unsupported network layer protocols.
- DHCP Client, Server and Relay
- RIP I and RIP II

IP Policy Routing

IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator.

Call Scheduling

Configure call time periods to allow and restrict access to remote nodes.

Networking Compatibility

Your Prestige is compatible with the major ADSL DSLAM (Digital Subscriber Line Access Multiplexer) providers, making configuration as simple as possible for you.

Multiplexing

Your Prestige supports VC-based and LLC-based multiplexing.

Encapsulation

The Prestige supports RFC 1483 encapsulation over ATM and PPP over Ethernet (RFC 2516).

SNMP

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. The Prestige supports SNMP version one (SNMPv1) and version two (SNMPv2).

Network Address Translation (NAT)

Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).

Full Network Management

- SNMP (Simple Network Management Protocol) support.
- SMT (System Management Terminal) through a telnet connection.

- Web configurator.

PAP and CHAP Security

The Prestige supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure since the password is scrambled prior to transmission. However, PAP is readily available on more platforms.

Filters

The Prestige's packet filtering functions allow added network security and management.

Reset Button

The Prestige comes with a reset button built into the rear panel. Use this button to restore the factory default password to 1234, IP address to 192.168.1.1, subnet mask to 255.255.255.0 and DHCP server enabled with a pool of 32 IP addressed starting at 192.168.1.33.

1.3 Applications for the Prestige

Here are some example uses for which the Prestige is well suited.

1.3.1 Internet Access

The Prestige is the ideal high-speed Internet access solution. Your Prestige supports the TCP/IP protocol, which the Internet uses exclusively. It is compatible with all major ADSL DSLAM providers. A DSLAM is a rack of ADSL line cards with data multiplexed into a backbone network interface/connection (e.g., T1, OC3, DS3, ATM or Frame Relay). Think of it as the equivalent of a modem rack for ADSL. A typical Internet Access application is shown next.

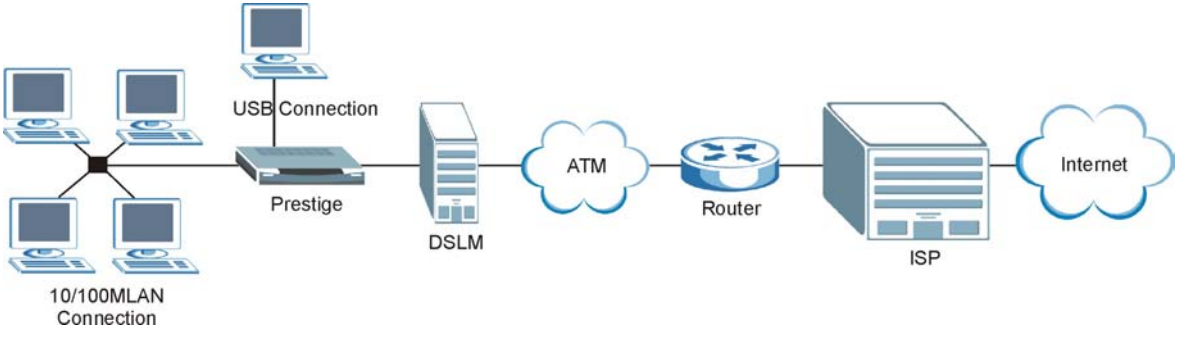


Figure 1-1 Internet Access Application

1.3.2 LAN to LAN Application

You can use the Prestige to connect two geographically dispersed networks through an ADSL line. A typical LAN-to-LAN application for your Prestige is shown as follows.

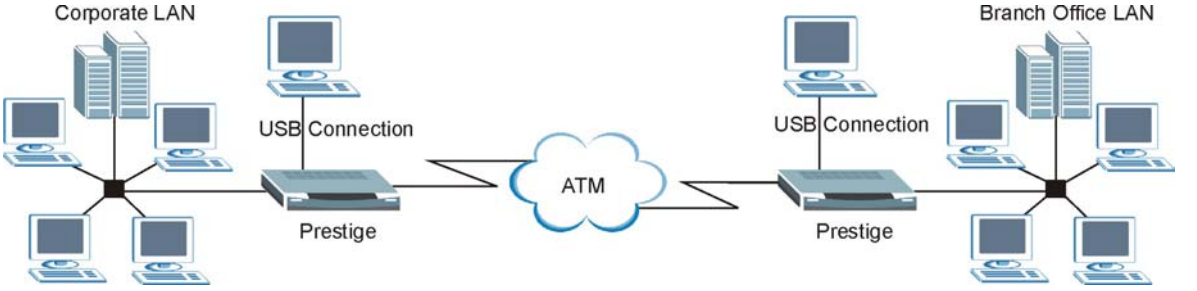


Figure 1-2 LAN-to-LAN Application

Chapter 2
Introducing the Web Configurator

This chapter describes how to access and navigate the web configurator.

2.1 Web Configurator Overview

The embedded web configurator (ewc) allows you to manage the Prestige from anywhere through a browser such as Microsoft Internet Explorer or Netscape Navigator. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions with JavaScript enabled. It is recommended that you set your screen resolution to 1024 by 768 pixels

2.2 Accessing the Prestige Web Configurator

Step 1. Make sure your Prestige hardware is properly connected (refer to Quick Start Guide).

Step 2. Prepare your computer/computer network to connect to the Prestige (refer to Quick Start Guide).

Step 3. Launch your web browser.

Step 4. Type "192.168.1.1" as the URL.

Step 5. An **Enter Network Password** window displays. Enter the user name ("admin" is the default), password ("1234" is the default) and click **OK**.

Figure 2-1 Password Screen

Step 6. You should now see the **Site Map** screen.

The Prestige automatically times out after five minutes of inactivity. Simply log back into the Prestige if this happens to you.

2.3 Navigating the Prestige Web Configurator

The following summarizes how to navigate the web configurator from the **Site Map** screen. Screens vary slightly for different Prestige models.

- Click **Wizard Setup** to begin a series of screens to configure your Prestige for the first time.
- Click a link under **Advanced Setup** to configure advanced Prestige features.
- Click a link under **Maintenance** to see Prestige performance statistics, upload firmware and back up, restore or upload a configuration file.
- Click **SITE MAP** to go to the **Site Map** screen.
- Click **Logout** in the navigation panel when you have finished a Prestige management session.

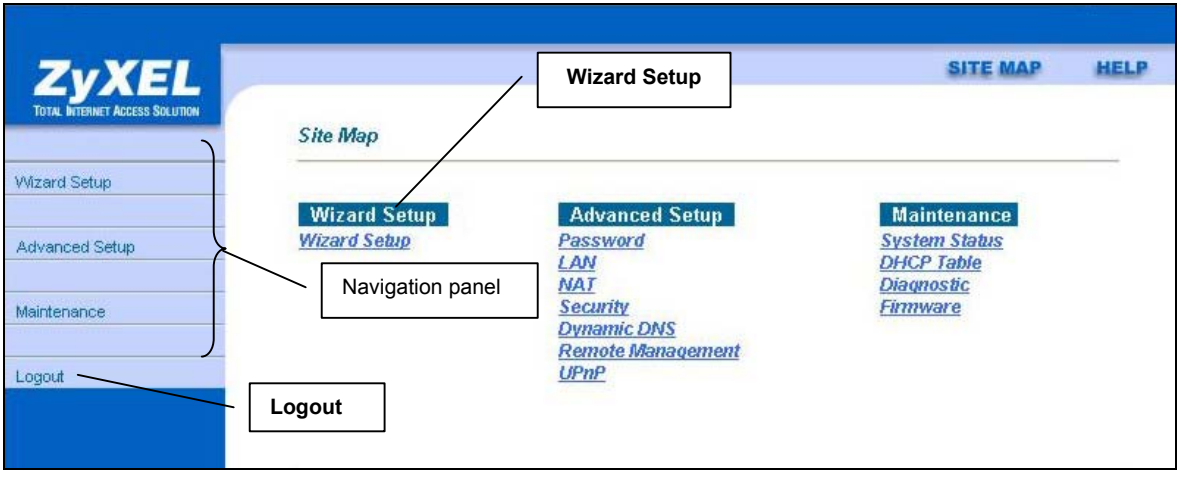


Figure 2-2 Web Configurator SITE MAP Screen

Click the HELP icon (located in the top right corner of most screens) to view embedded help.

2.4 Configuring Password

It is highly recommended that you change the password for accessing the Prestige.

To change your Prestige's password, click **Advanced Setup** and then **Password**. The screen appears as shown.

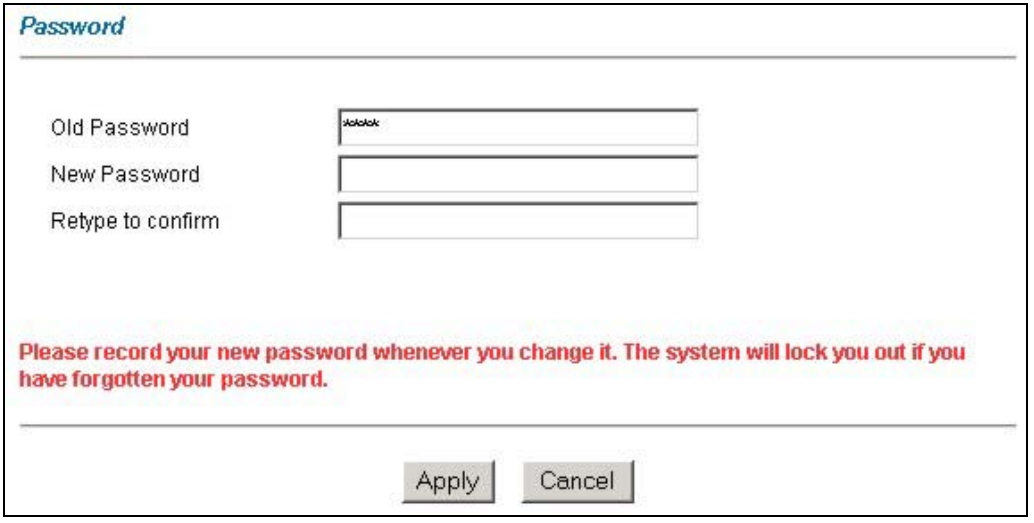

Password
Old Password
New Password
Retype to confirm
Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.
Apply
Cancel

Figure 2-3 Password

The following table describes the labels in this screen.

Table 2-1 Password

LABEL	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type the new password in this field.
Retype to Confirm	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

2.5 Resetting the Prestige

If you forget your password or cannot access the Prestige, you will need to reload the factory-default configuration file or use the **RESET** button the back of the Prestige. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously. The password will be reset to "1234", also.

2.5.1 Using The Reset Button

Make sure the **PWR** LED is on (not blinking) when you begin this procedure.

1. Press the **RESET** button for more than five seconds, then release it. If the **PWR** LED begins to blink, the defaults have been restored and the Prestige restarts. Otherwise, go to step 2.
2. Turn the Prestige off.
3. While pressing the **RESET** button, turn the Prestige on.

Continue to hold the **RESET** button. The **PWR** LED will begin to blink and flicker very quickly after about 10 or 15 seconds. This indicates that the defaults have been restored and the Prestige is now restarting.

Chapter 3
Wizard Setup

This chapter provides information on the Wizard Setup screens in the web configurator.

3.1 Wizard Setup Introduction

Use the Wizard Setup screens to configure your system for Internet access settings and fill in the fields with the information in the *Internet Account Information* table of the *Quick Start Guide*. Your ISP may have already configured some of the fields in the wizard screens for you.

3.2 Encapsulation

Be sure to use the encapsulation method required by your ISP. The Prestige supports the following methods.

3.2.1 PPPoE Encapsulation

PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP. The Prestige bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) that connects to an ADSL Access Concentrator where the PPP session terminates. One PVC can support any number of PPP sessions from your LAN. The **PPPoE** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the Prestige (rather than individual computers), the computers on the

LAN do not need PPPoE software installed, since the Prestige does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

3.2.2 RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to the RFC for more detailed information.

3.3 Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

3.3.1 VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

3.3.2 LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

3.4 VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the appendix for more information.

3.5 Wizard Setup Configuration: First Screen

In the **SITE MAP** screen click **Wizard Setup** to display the first wizard screen.

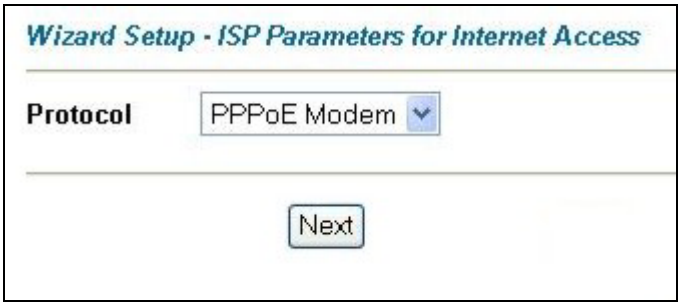


Figure 3-1 Wizard Screen 1

The following table describes the labels in this screen.

Table 3-1 Wizard Screen 1

LABEL	DESCRIPTION
Protocol	Select the encapsulation type your ISP uses from the drop-down list box. Choose from: **PPPoE Modem** - A dial up connection that uses PPPoE encapsulation and requires a username and password. **Modem** - An always-up connection that uses the RFC1483 protocol.
Next	Click this button to go to the next wizard screen. The next wizard screen you see depends on what protocol you chose above.

3.6 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the Prestige. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number

unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your Prestige, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Prestige will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Prestige unless you are instructed to do otherwise.

3.7 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and ENET ENCAP Gateway.

3.7.1 IP Assignment with PPPoE Encapsulation

If you have a dynamic IP, then the IP address and ENET ENCAP Gateway fields are not applicable (N/A). If you have a static IP, then you *only* need to fill in the IP Address field and *not* the ENET ENCAP Gateway field.

3.7.2 IP Assignment with RFC 1483 Encapsulation

In this case the IP Address Assignment *must* be static with the same requirements for the IP Address and ENET ENCAP Gateway fields as stated above.

3.7.3 Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

```
10.0.0.0      —  10.255.255.255
172.16.0.0    —  172.31.255.255
192.168.0.0   —  192.168.255.255
```

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

3.8 NAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

3.9 Wizard Setup Configuration: Second Screen

The second wizard screen varies depending on what mode and encapsulation type you use. All screens shown are with routing mode. Configure the fields and click **Next** to continue.

3.9.1 RFC 1483

Select **RFC 1483** from the **Encapsulation** drop-down list box in the first wizard screen to display the screen as shown.

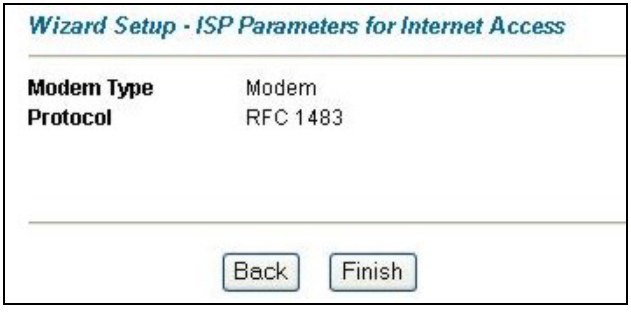


Figure 3-2 Internet Connection with RFC 1483

The following table describes the labels in this screen.

Table 3-2 Internet Connection with RFC 1483

LABEL	DESCRIPTION
Modem Type	This field displays the protocol selected on the previous wizard screen.
Protocol	This field displays the encapsulation used by the protocol selected on the previous wizard screen.
Back	Click **Back** to go back to the first wizard screen.
Finish	Click **Finish** to save and complete the wizard setup.

3.9.2 PPPoE

Select **PPPoE** from the **Encapsulation** drop-down list box in the first wizard screen to display the screen as shown.

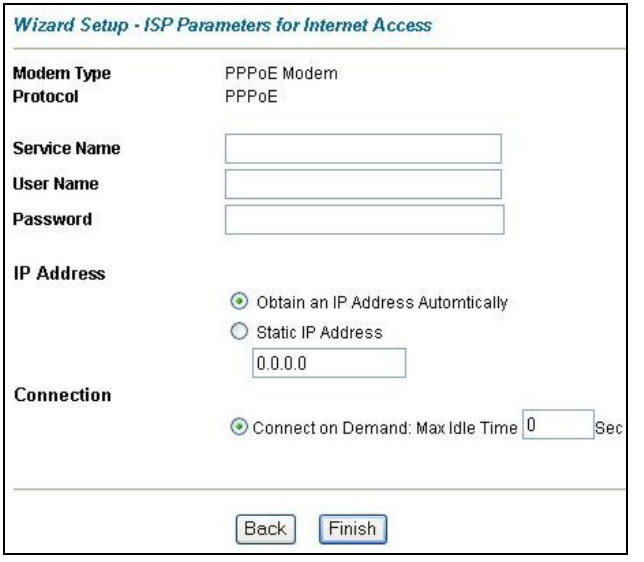


Figure 3-3 Internet Connection with PPPoE

The following table describes the labels in this screen.

Table 3-3 Internet Connection with PPPoE

LABEL	DESCRIPTION
Modem Type	This field displays the protocol selected in the previous wizard screen.
Protocol	This field displays the encapsulation used for the protocol selected in the previous wizard screen.
Service Name	Type the name of your PPPoE service here.
User Name	Configure **User Name** and **Password** fields for **PPPoE** encapsulation only. Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. The Single User Account feature can be used with either a dynamic or static IP address. Select **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the **IP Address** text box below.
Connection	**Connect on Demand: Max. Idle Time** specifies an idle time-out (in seconds). The default setting for this field is, which means the Internet session does not timeout. The schedule rule(s) in SMT menu 26 has priority over your **Connection** settings.
Back	Click **Back** to go back to the first wizard screen.
Finish	Click **Finish** to save and complete the wizard setup.

3.10 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Prestige as a DHCP server or disable it. When configured as a server, the Prestige provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

3.10.1 IP Pool Setup

The Prestige is pre-configured with a pool of IP addresses. This leaves a plurality of IP addresses, (excluding the Prestige itself which has a default IP of 192.168.1.1) for other server machines, for example, server for mail, FTP, telnet, web, etc., that you may have.

Congratulations ! Your Web Configurator Internet Access Configuration is done.
You should be able to access the Internet now. You can try it by going to the ZyXEL home page at http://www.zyxel.com.

Figure 4 Setup Complete

3.11 Test Your Internet Connection

Launch your web browser and navigate to www.zyxel.com. Internet access is just the beginning. Refer to the rest of this *User's Guide* for more detailed information on the complete range of Prestige features. If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the Wizard Setup are correct.

Part II:

LAN

This part covers LAN (Local Area Network) setup.

Chapter 4
LAN Setup

This chapter describes how to configure LAN settings.

4.1 LAN Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

4.1.1 LANs, WANs and the Prestige

The actual physical connection determines whether the Prestige ports are LAN or WAN ports. There are two separate IP networks, one inside, the LAN network; the other outside: the WAN network as shown next:

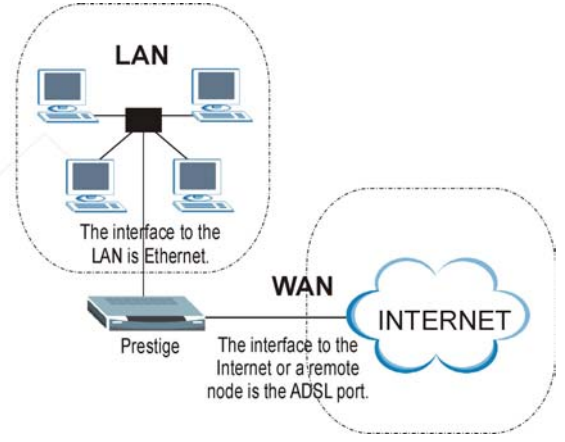

LAN
The interface to the LAN is Ethernet.
WAN
INTERNET
Prestige
The interface to the Internet or a remote node is the ADSL port.

Figure 4-1 LAN and WAN IP Addresses

4.2 DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, for example, the IP address of *www.zyxel.com* is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. If your ISP gives you the DNS server addresses, enter them in the **DNS Server** fields in **DHCP Setup**, otherwise, leave them blank.

Some ISP's choose to pass the DNS servers using the DNS server extensions of PPP IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The Prestige supports the IPCP DNS server extensions through the DNS proxy feature.

If the **Primary** and **Secondary DNS Server** fields in **DHCP Setup** are not specified, for instance, left as 0.0.0.0, the Prestige tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the Prestige, the Prestige forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** menu. This way, the Prestige can pass the DNS servers to the computers and the computers can query the DNS server directly without the Prestige's intervention.

4.3 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

There are two ways that an ISP disseminates the DNS server addresses.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in DHCP Setup.
2. Leave the DNS Server fields in DHCP Setup blank (for example 0.0.0.0). The Prestige acts as a DNS proxy when this field is blank.

4.4 LAN TCP/IP

The Prestige has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

4.4.1 Factory LAN Defaults

The LAN parameters of the Prestige are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

4.4.2 IP Address and Subnet Mask

Refer to the *IP Address and Subnet Mask* section in the **Wizard Setup** chapter for this information.

4.4.3 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

1. **Both -** the Prestige will broadcast its routing table periodically and incorporate the RIP information that it receives.
2. **In Only -** the Prestige will not send any RIP packets but will accept all RIP packets received.
3. **Out Only -** the Prestige will send out RIP packets but will not accept any RIP packets received.
4. **None -** the Prestige will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the Prestige sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.

4.4.4 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The Prestige supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the Prestige queries all directly connected networks to gather group membership. After that, the Prestige periodically updates this information. IP multicasting can be enabled/disabled on the Prestige LAN interface in the web configurator. Select **None** to disable IP multicasting.

4.5 Configuring LAN

Click **LAN** to open the following screen.

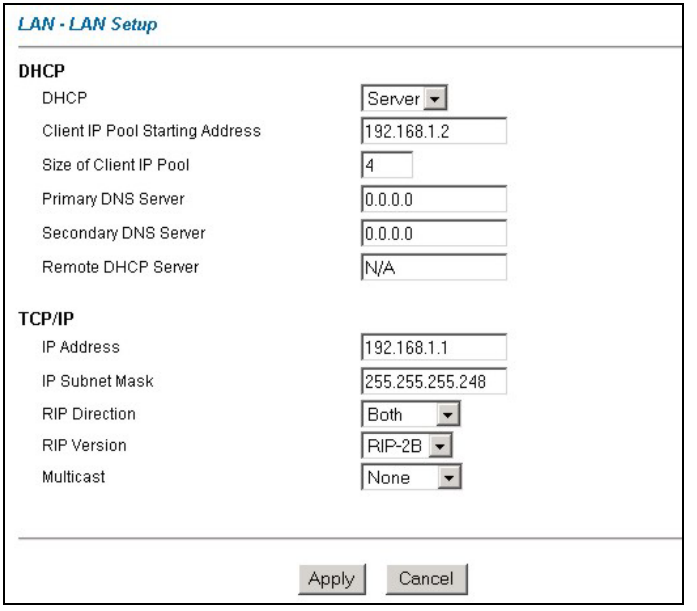


Figure 4-2 LAN

The following table describes the labels in this screen.

Table 4-1 LAN

LABEL	DESCRIPTION
DHCP	
DHCP	If set to **Server**, your Prestige can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to **None**, the DHCP server will be disabled. If set to **Relay**, the Prestige acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case. When DHCP is used, the following items need to be set:

Table 4-1 LAN

LABEL	DESCRIPTION
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Secondary DNS Server	As above.
Remote DHCP Server	If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here.
TCP/IP	
IP Address	Enter the IP address of your Prestige in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
RIP Direction	Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**.
RIP Version	Select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group. The Prestige supports both IGMP version 1 (**IGMP-v1**) and **IGMP-v2**. Select **None** to disable it.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

Part III:

NAT and Dynamic DNS

This part covers NAT (Network Address Translation) and dynamic DNS (Domain Name Sever).

Chapter 5
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

5.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

5.2 Single User Account Server (SUA Server)

Typically, if there are multiple users on the LAN wanting to concurrently access the Internet, you will have to lease a block of legal, or globally unique, IP addresses from the ISP.

The Single User Account (SUA) feature allows you to have the same benefits as having multiple legal addresses, but only pay for one IP address, thus saving significantly on the subscription fees. (Check with your ISP before you enable this feature).

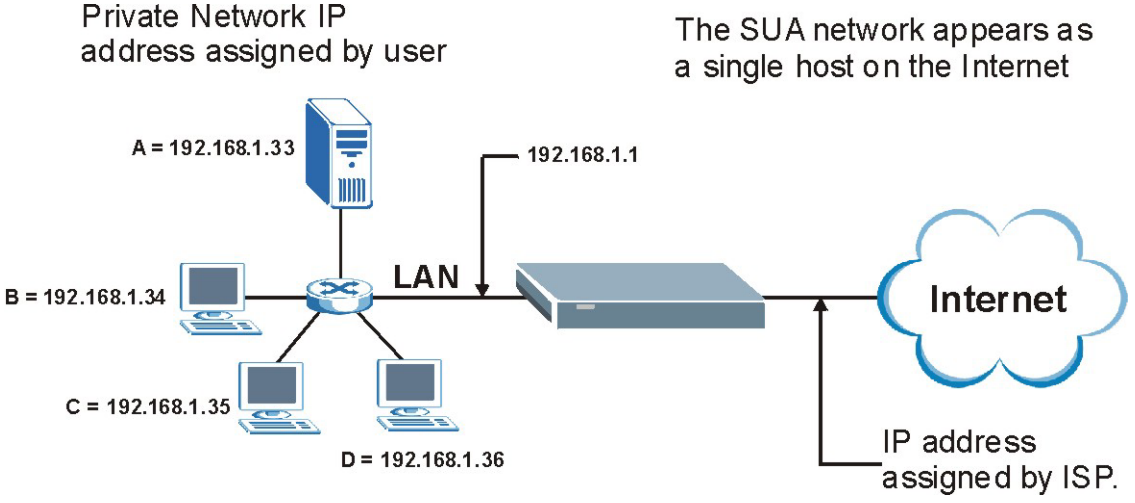


Figure 5-1 Single User Account Topology

The Single User Account feature may also be used on connections to remote networks other than the ISP. For example, this feature can be used to simplify the allocation of IP addresses when connecting branch offices to the corporate network.

The IP address for the SUA can be either fixed or dynamically assigned when a call is connected. In addition, you can designate servers, e.g., a web server and a telnet server, on your local network and make them accessible to the outside world.

If you do not define any server, SUA offers the additional benefit of firewall protection. If no server is defined, all incoming inquiries are filtered by your Prestige, thus preventing intruders from probing your network.

Your Prestige accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. For more information on IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

5.2.1 Advantages of SUA

In summary:

- SUA is a cost-effective solution for small offices with less than 20 hosts to access the Internet or other remote TCP/IP networks.
- SUA supports servers to be accessible to the outside world.
- SUA can provide firewall protection if you do not specify a server. All incoming inquiries will be filtered out by your Prestige.
- UDP and TCP packets can be routed. In addition, partial ICMP, including echo and trace route, is supported.

5.2.2 Configuring Inside Servers

The Prestige enables you to make inside servers for different services, e.g., web or FTP, visible to the outside users, even though SUA makes your whole inside network appear as a single machine to the outside world. The port number identifies a service, e.g., web service is on port 80 and FTP on port 21.

Let's say you want to assign ports 22-25 to one server, port 80 to another and assign a default server IP address of 192.168.1.35 as shown in the next figure.

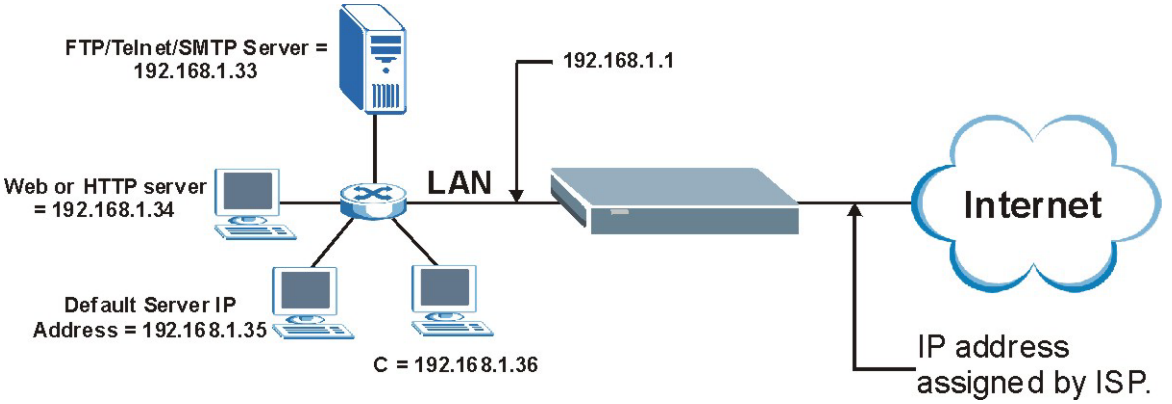


Figure 5-2 Multiple Servers Behind NAT Example

Please note that a server can support more than one service, e.g., a server can provide both FTP and DNS service, while another provides only web service. Also, since you need to specify the IP address of a server in the Prestige, a server must have a fixed IP address and not be a DHCP client whose IP address potentially changes each time it is powered on.

In addition to the servers for specific services, SUA supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default server is not defined, the service request is simply discarded.

The most often used port numbers are described in the following table:

Table 5-1 NAT Mode

SERVICES	PORT NUMBER
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS(Domain Name System)	53
HTTP (Hyper Text Transfer Protocol or WWW, Web)	80
PPTP (Point-to-Point Tunneling Protocol)	1723

5.3 Selecting the NAT Mode

Click **NAT** to open the following screen.

Figure 5-3 NAT Mode

The following table describes the labels in this screen.

Table 5-2 NAT Mode

LABEL	DESCRIPTION
None	Select this radio button to disable NAT.
SUA Only	Select this radio button if you have just one public WAN IP address for your Prestige. The Prestige uses Address Mapping Set 1 in the **NAT - Edit SUA/NAT Server Set** screen.
Edit Details	Click this link to go to the **NAT - Edit SUA/NAT Server Set** screen.
Apply	Click **Apply** to save your configuration.

5.4 Configuring SUA Server

If you do not assign an IP address in Server Set **1 (default server), the Prestige discards all packets received for ports that are not specified here or in the remote management setup.**

Click **NAT**, Select **SUA Only** and click **Edit Details** to open the following screen.

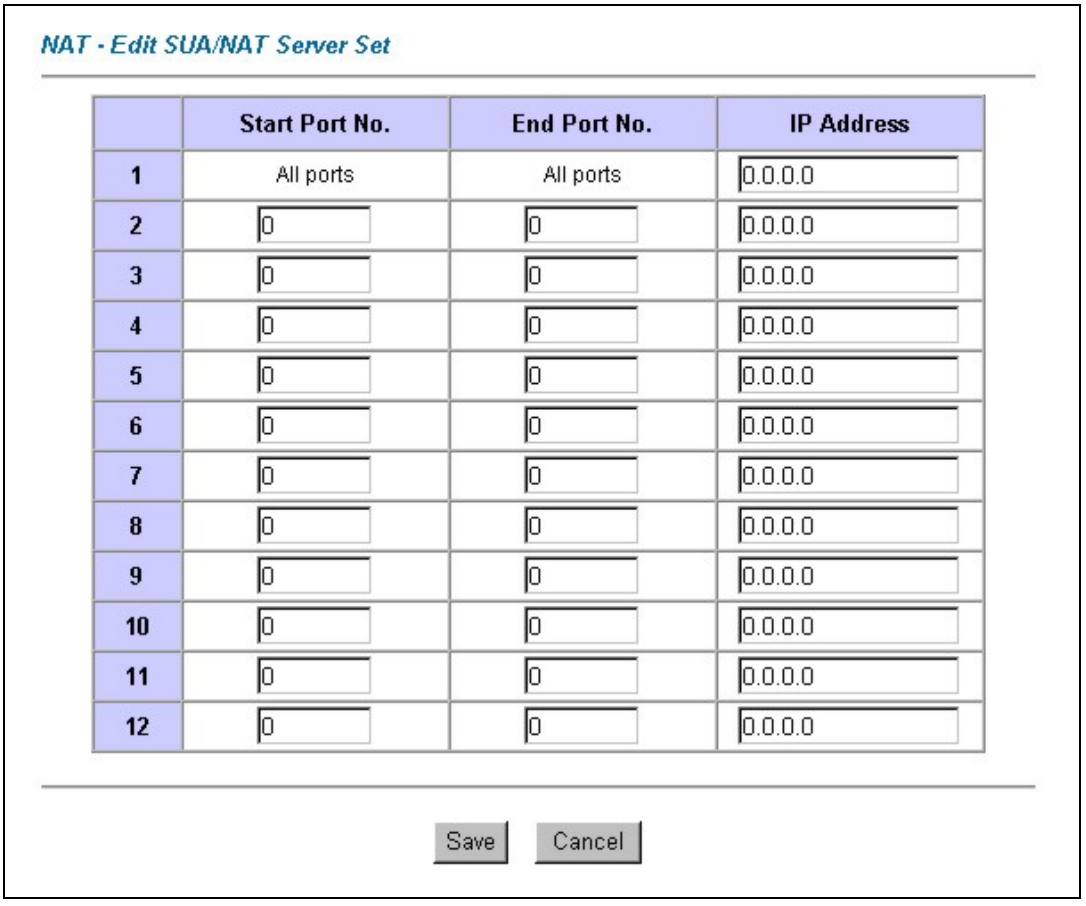


Figure 5-4 Edit SUA/NAT Server Set

The following table describes the labels in this screen.

Table 5-3 Edit SUA/NAT Server Set

LABEL	DESCRIPTION
Start Port No.	Enter a port number in this field. To forward only one port, enter the port number again in the **End Port No.** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port No.** field.
End Port No.	Enter a port number in this field. To forward only one port, enter the port number again in the **Start Port No.** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **Start Port No.** field above.
IP Address	Enter your server IP address in this field.
Save	Click **Save** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previous configuration.

Chapter 6
Dynamic DNS Setup

This chapter discusses how to configure your Prestige to use Dynamic DNS.

6.1 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

6.1.1 DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

6.2 Configuring Dynamic DNS

To change your Prestige's DDNS, click **Dynamic DNS**. The screen appears as shown.

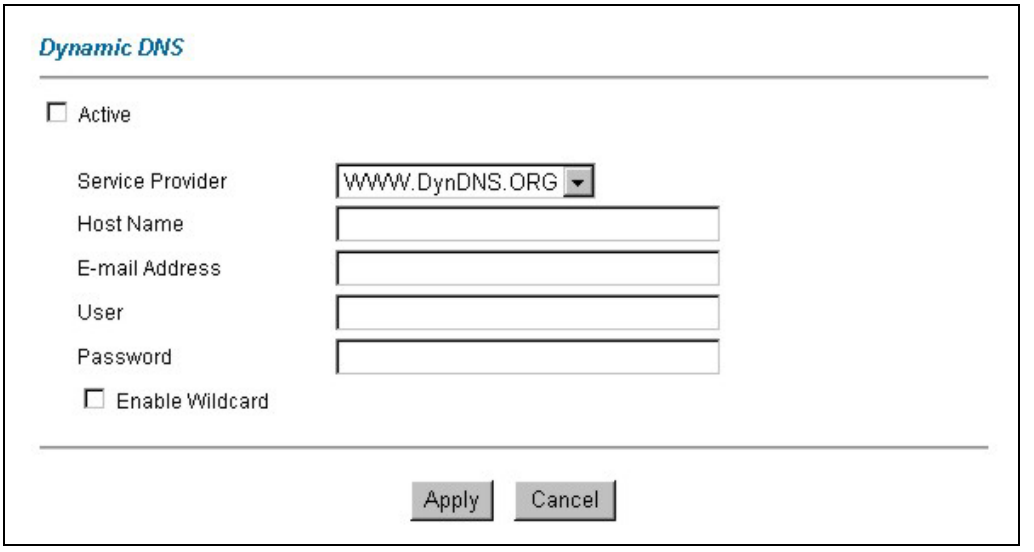


Figure 6-1 DDNS

The following table describes the labels in this screen.

Table 6-1 DDNS

LABEL	DESCRIPTION
Active	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your Prestige by your Dynamic DNS provider.
E-mail Address	Type your e-mail address.
User	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard	Select this check box to enable DYNDNS Wildcard.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previously saved settings.

Part IV:

Remote Management and UPnP

This part contains information on how to configure the Prestige for remote management and setting up Universal Plug and Play (UPnP).

Chapter 7
Remote Management Configuration

This chapter provides information on configuring remote management. Remote management is not available on all models

7.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which Prestige interface (if any) from which computers.

You may manage your Prestige from a remote location via:

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only
- Neither (Disable)

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

7.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in one of the remote management screens.
3. The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
4. There is an SMT console session running.
5. There is already another remote management session of the same type (web, FTP or Telnet) running. You may only have one remote management session of the same type running at one time.
6. There is a web remote management session running with a Telnet session. A web session will be disconnected if you begin a Telnet session; it will not begin if there already is a Telnet session.

7.1.2 Remote Management and NAT

When NAT is enabled:

- Use the Prestige's WAN IP address when configuring from the WAN.
- Use the Prestige's LAN IP address when configuring from the LAN.

7.1.3 System Timeout

There is a system timeout of five minutes (three hundred seconds) for either the console port or telnet/web/FTP connections. Your Prestige automatically logs you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

7.2 Telnet

You can configure your Prestige for remote Telnet access as shown next.

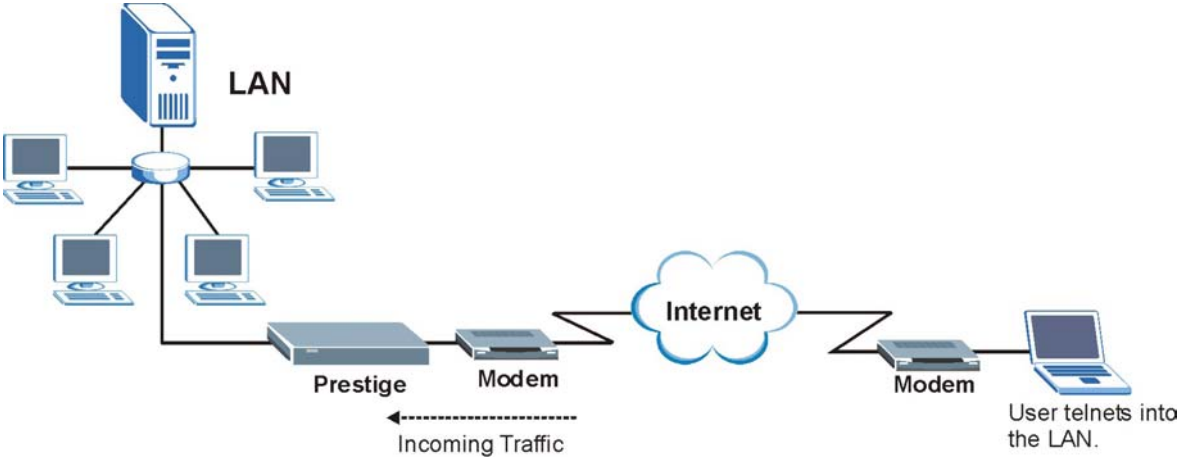


Figure 7-1 Telnet Configuration on a TCP/IP Network

7.3 FTP

You can upload and download Prestige firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

7.4 Web

You can use the Prestige's embedded web configurator for configuration and file management. See the online help for details.

7.5 Configuring Remote Management

Click **Remote Management** to open the following screen.

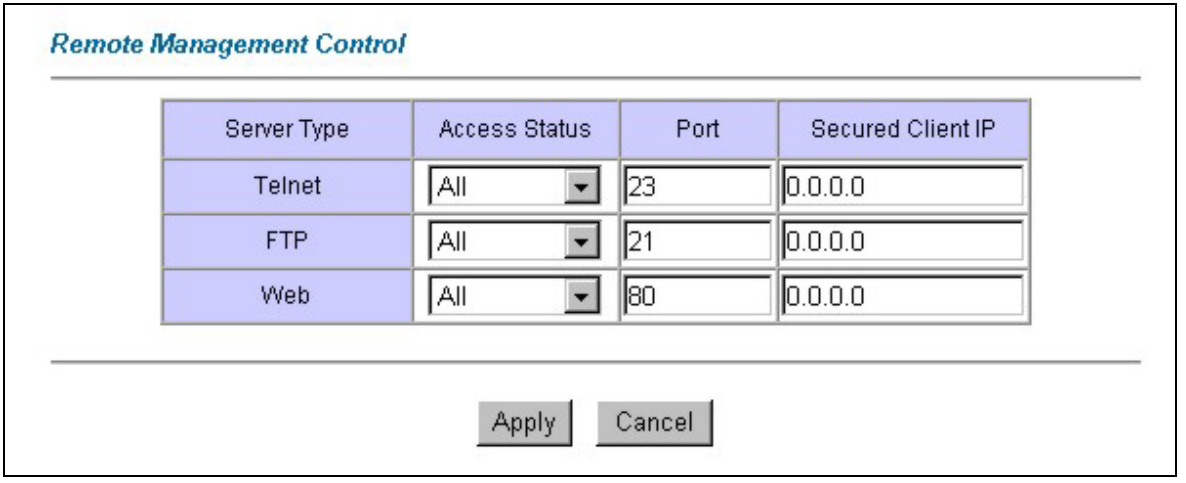


Figure 7-2 Remote Management

The following table describes the labels in this screen.

Table 7-1 Remote Management

LABEL	DESCRIPTION
Server Type	Each of these labels denotes a service that you may use to remotely manage the Prestige.
Access Status	Select the access interface. Choices are **All**, **LAN Only**, **WAN Only** and **Disable**.
Port	This field shows the port number for the remote management service. You may change the port number for a service in this field, but you must use the same port number to use that service for remote management.

Table 7-1 Remote Management

LABEL	DESCRIPTION
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the Prestige. Type an IP address to restrict access to a client with a matching IP address.
Apply	Click **Apply** to save your settings back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 8
Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

8.1 Universal Plug and Play Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

8.1.1 How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

8.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the *Network Address Translation (NAT)* chapter for further information about NAT.

8.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

8.2 UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing ZyXEL's UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger 5.0 and Xbox are still being tested.

UPnP broadcasts are only allowed on the LAN.

See later sections for examples of installing UPnP in Windows XP and Windows Me as well as an example of using UPnP in Windows.

8.2.1 Configuring UPnP

From the **Site Map** in the main menu, click **UPnP** under **Advanced Setup** to display the screen shown next.

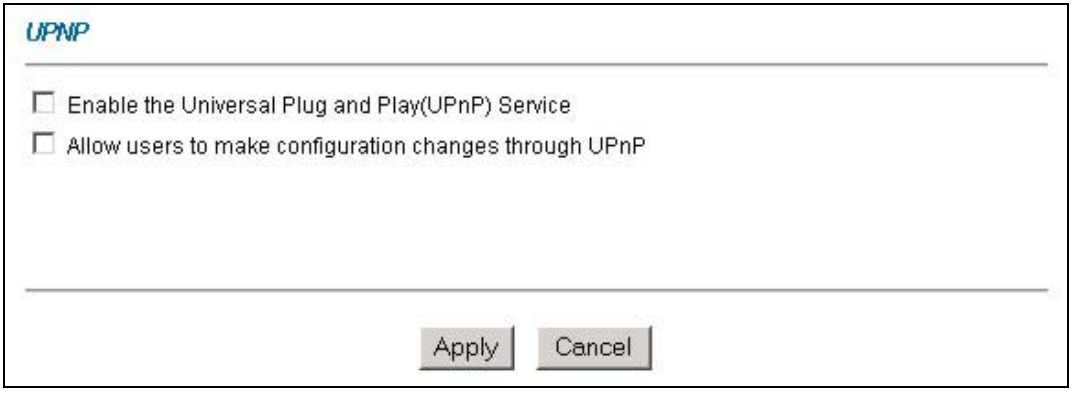


Figure 8-1 Configuring UPnP

The following table describes the labels in this screen.

Table 8-1 Configuring UPnP

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Service	Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the Prestige's IP address (although you must still enter the password to access the web configurator).

Table 8-1 Configuring UPnP

LABEL	DESCRIPTION
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the Prestige so that they can communicate through the Prestige, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Apply	Click **Apply** to save the setting to the Prestige.
Cancel	Click **Cancel** to return to the previously saved settings.

8.3 Installing UPnP in Windows Example

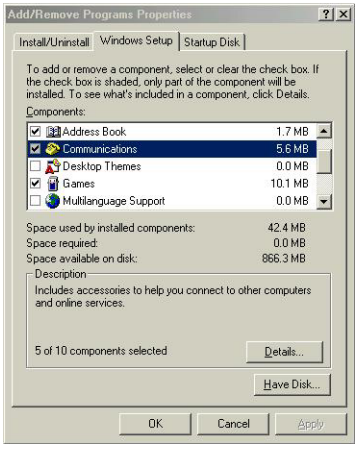
This section shows how to install UPnP in Windows Me and Windows XP.

8.3.1 Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

Step 1. Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

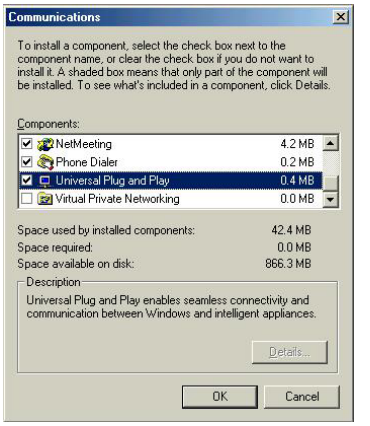
Step 2. Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.


Add/Remove Programs Properties
Install/Uninstall
Windows Setup
Startup Disk
To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.
Components:
Address Book 1.7 MB
Communications 5.6 MB
Desktop Themes 0.0 MB
Games 10.1 MB
Multilanguage Support 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Includes accessories to help you connect to other computers and online services.
5 of 10 components selected
Details...
Have Disk...
OK
Cancel
Apply

Step 3. In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Step 4. Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

Step 5. Restart the computer when prompted.


Communications
To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
NetMeeting 4.2 MB
Phone Dialer 0.2 MB
Universal Plug and Play 0.4 MB
Virtual Private Networking 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.
Details...
OK
Cancel

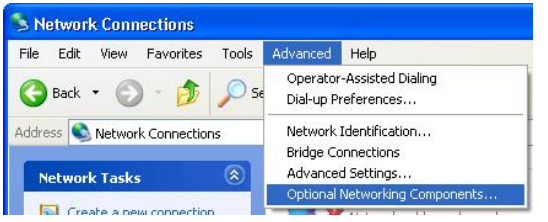
8.3.2 Installing UPnP in Windows XP

Follow the steps below to install the UPnP in Windows XP.

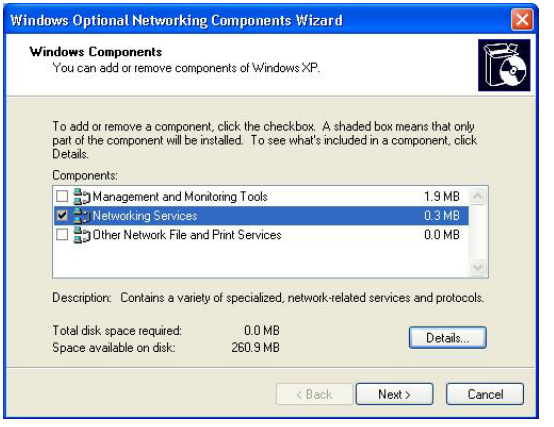
Step 1. Click **Start** and **Control Panel**.

Step 2. Double-click **Network Connections**.

Step 3. In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.
The **Windows Optional Networking Components Wizard** window displays.

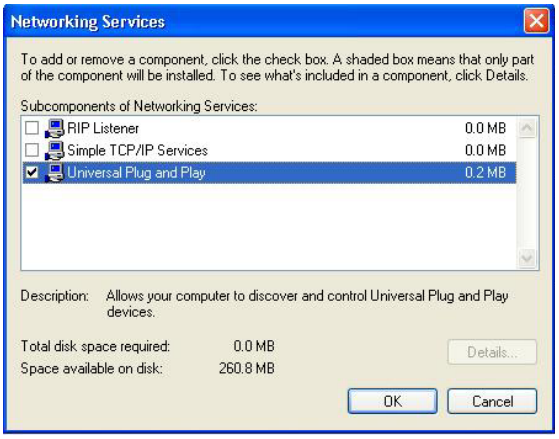


Step 4. Select **Networking Service** in the **Components** selection box and click **Details**.


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 1.9 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 260.9 MB
Details...
< Back
Next >
Cancel

Step 5. In the **Networking Services** window, select the **Universal Plug and Play** check box.

Step 6. Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
Universal Plug and Play 0.2 MB
Description: Allows your computer to discover and control Universal Plug and Play devices.
Total disk space required: 0.0 MB
Space available on disk: 260.8 MB
Details...
OK
Cancel

8.4 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the Prestige.

Make sure the computer is connected to a LAN port of the Prestige. Turn on your computer and the Prestige.

8.4.1 Auto-discover Your UPnP-enabled Network Device

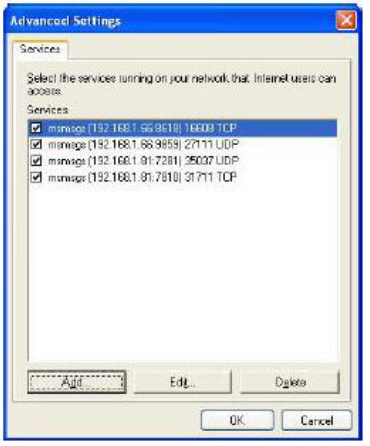
Step 1. Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

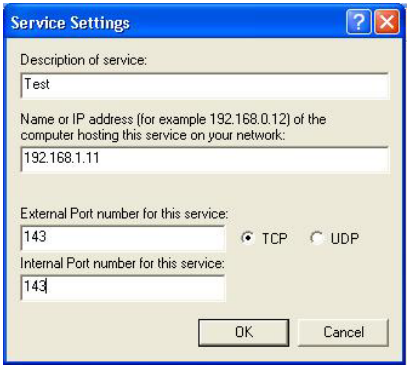
Step 2. Right-click the icon and select **Properties**.

Step 3. In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Internet Connection Properties
General
Connect to the Internet using:
Internet Connection
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel

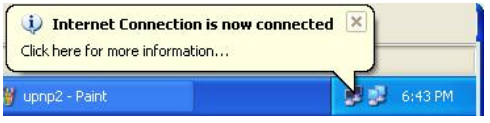
Step 4. You may edit or delete the port mappings or click **Add** to manually add port mappings.



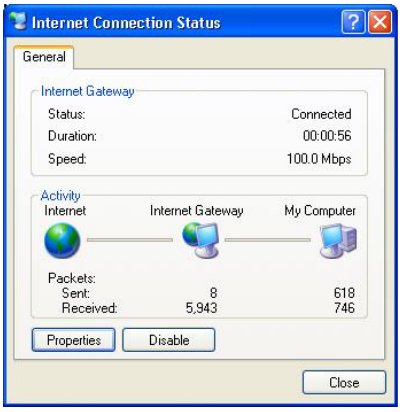


When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

Step 5. Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray



Step 6. Double-click on the icon to display your current Internet connection status.



8.4.2 Web Configurator Easy Access

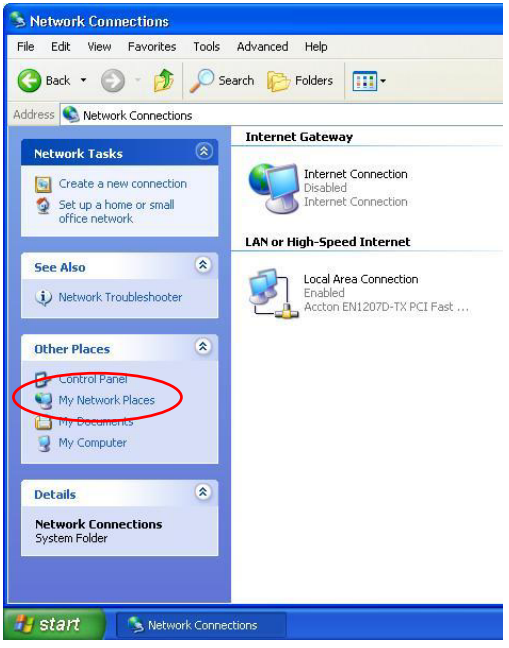
With UPnP, you can access the web-based configurator on the Prestige without finding out the IP address of the Prestige first. This comes helpful if you do not know the IP address of the Prestige.

Follow the steps below to access the web configurator.

Step 1. Click **Start** and then **Control Panel**.

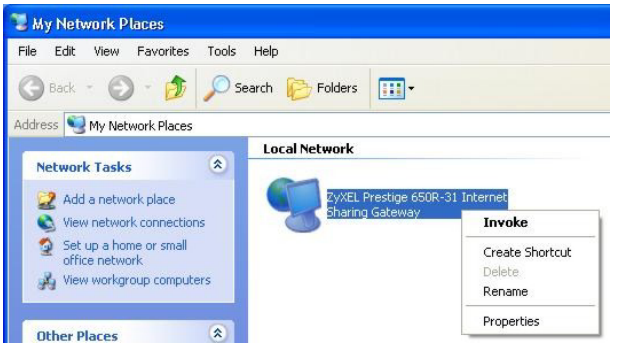
Step 2. Double-click **Network Connections**.

Step 3. Select **My Network Places** under **Other Places**.



Step 4. An icon with the description for each UPnP-enabled device displays under **Local Network**.

Step 5. Right-click on the icon for your Prestige and select **Invoke**. The web configurator login screen displays.



Step 6. Right-click on the icon for your Prestige and select **Properties**. A properties window displays with basic information about the Prestige.

Part V:

Maintenance

This part covers the maintenance screens.

Chapter 9
Maintenance

This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.

9.1 Maintenance Overview

Use the maintenance screens to view system information, upload new firmware, manage configuration and restart your Prestige.

9.2 System Status Screen

Click **System Status** to open the following screen, where you can use to monitor your Prestige. Note that these fields are READ-ONLY and are meant to be used for diagnostic purposes.

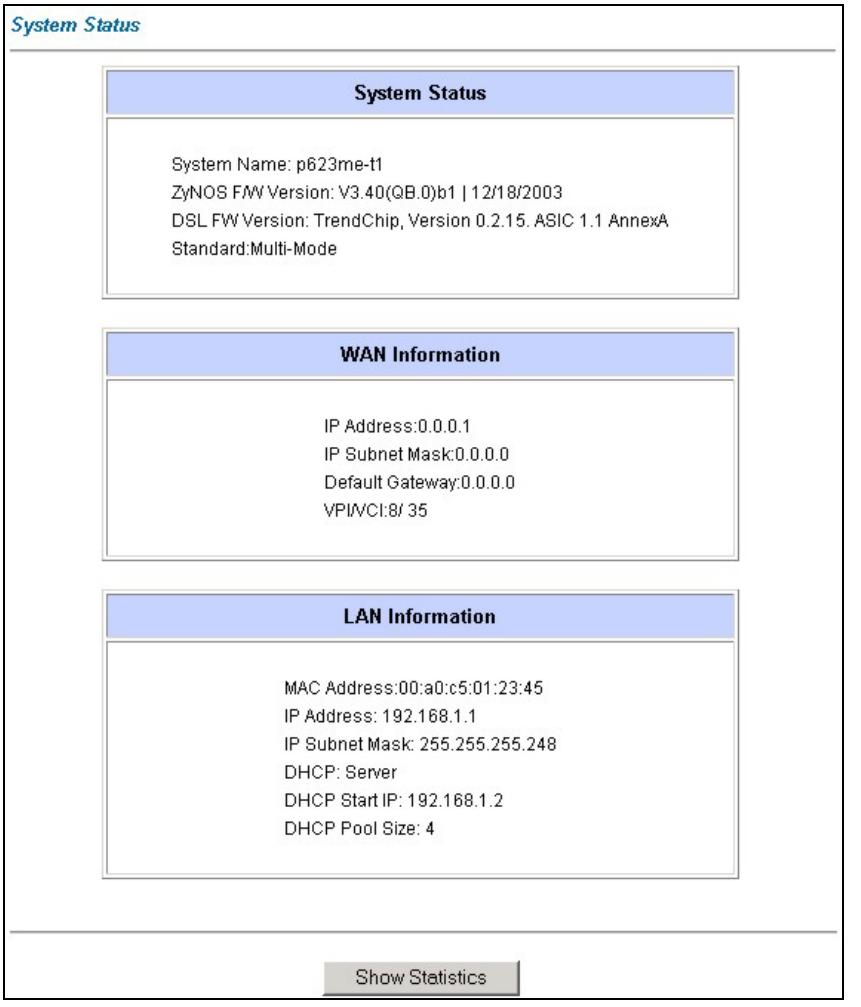


Figure 9-1 System Status

The following table describes the labels in this screen.

Table 9-1 System Status

LABEL	DESCRIPTION
System Status	

Table 9-1 System Status

LABEL	DESCRIPTION
System Name	This is the name of your Prestige. It is for identification purposes.
ZyNOS F/W Version	This is the ZyNOS firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
DSL FW Version	This is the DSL firmware version associated with your Prestige.
Standard	This is the standard that your Prestige is using.
WAN Information	
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port IP subnet mask.
Default Gateway	This is the IP address of the default gateway, if applicable.
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the first Wizard screen.
LAN Information	
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your Prestige.
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port IP subnet mask.
DHCP	This is the WAN port DHCP role - **Server**, **Relay** (not all Prestige models) or **None**.
DHCP Start IP	This is the first of the contiguous addresses in the IP address pool.
DHCP Pool Size	This is the number of IP addresses in the IP address pool.
Show Statistics	Click **Show Statistics** to see router performance statistics such as number of packets sent and number of packets received for each port.

9.2.1 System Statistics

Click **Show Statistics** in the **System Status** screen to open the following screen. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

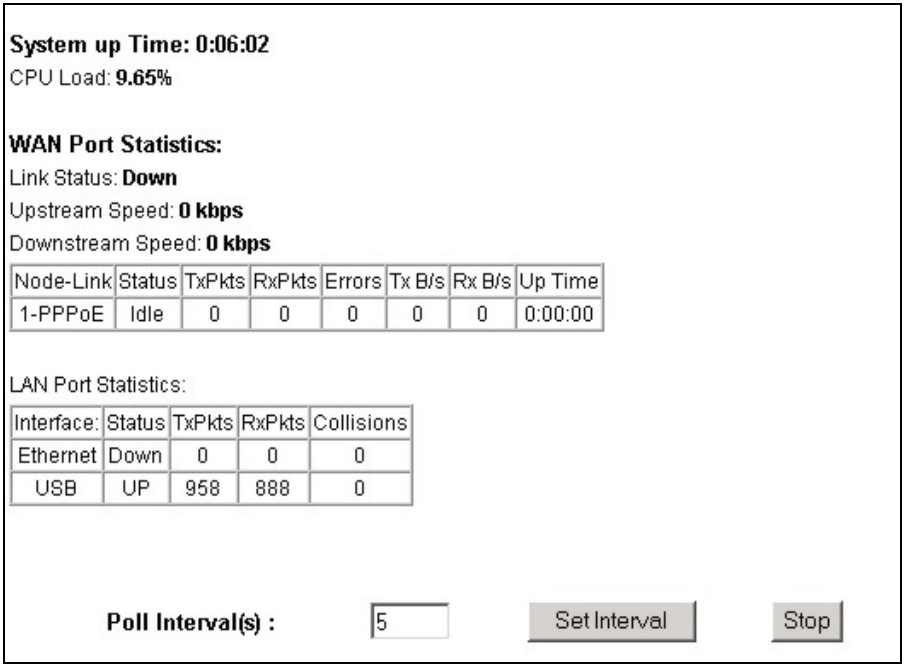

System up Time: 0:06:02
CPU Load: 9.65%
WAN Port Statistics:
Link Status: Down
Upstream Speed: 0 kbps
Downstream Speed: 0 kbps
Node-Link Status TxPkts RxPkts Errors Tx B/s Rx B/s Up Time
1-PPPoE Idle 0 0 0 0 0 0:00:00
LAN Port Statistics:
Interface: Status TxPkts RxPkts Collisions
Ethernet Down 0 0 0
USB UP 958 888 0
Poll Interval(s) :
5
Set Interval
Stop

Figure 9-2 System Status: Show Statistics

The following table describes the labels in this screen.

Table 9-2 System Status: Show Statistics

LABEL	DESCRIPTION
System up Time	This is the elapsed time the system has been up.
CPU Load	This field specifies the percentage of CPU utilization.
WAN Port Statistics	This is the WAN port.
Link Status	This is the status of your WAN link.

Table 9-2 System Status: Show Statistics

LABEL	DESCRIPTION
Upstream Speed	This is the upstream speed of your Prestige.
Downstream Speed	This is the downstream speed of your Prestige.
Node-Link	This field displays the remote node index number and link type. Link types are PPPoA, ENET, RFC 1483 and PPPoE.
Status	For the WAN port, this displays the port speed and duplex setting if you're using Ethernet encapsulation and **down** (line is down), **idle** (line (ppp) idle), **dial** (starting to trigger a call) and **drop** (dropping a call) if you're using PPPoE encapsulation. For a LAN port, this shows the port speed and duplex setting.
LAN Port Statistics	This is the LAN port.
Interface	This field displays the type of port.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Errors	This field displays the number of error packets on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the elapsed time this port has been up.
Collisions	This is the number of collisions on this port.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval** field above.
Stop	Click this button to halt the refreshing of the system statistics.

9.3 DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Prestige as a DHCP server or disable it. When configured as a server, the Prestige provides the TCP/IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **MAINTENANCE**, and then the **DHCP Table** tab. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the DHCP server.

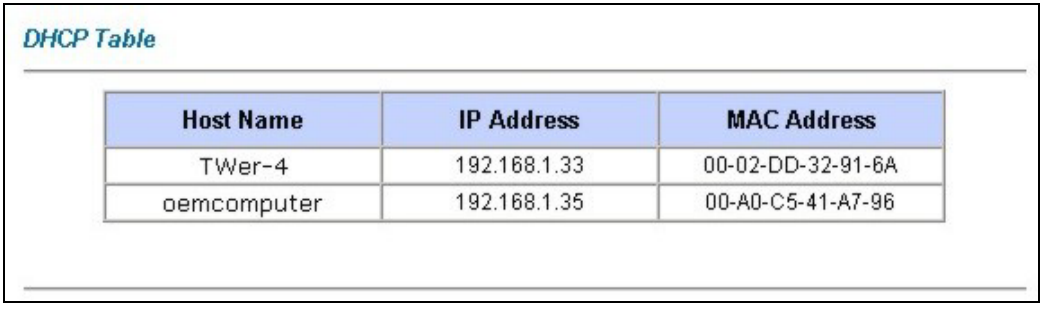


Figure 9-3 DHCP Table

The following table describes the labels in this screen.

Table 9-3 DHCP Table

LABEL	DESCRIPTION
Host Name	This is the name of the host computer.
IP Address	This field displays the IP address relative to the **Host Name** field.
MAC Address	This field displays the MAC (Media Access Control) address of the computer with the displayed host name. Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

9.4 Diagnostic Screens

These read-only screens display information to help you identify problems with the Prestige.

Click **Diagnostic** to display the following screen.

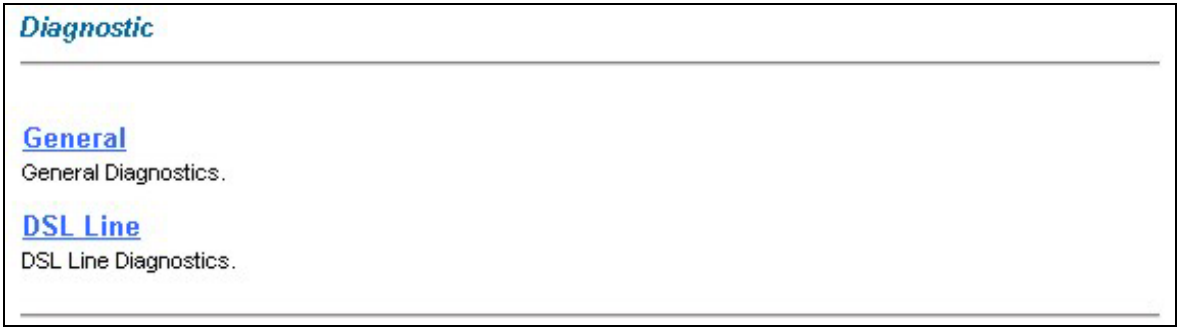


Figure 9-4 Diagnostic

9.4.1 Diagnostic General Screen

Click **Diagnostic** and then **General** to open the screen shown next.

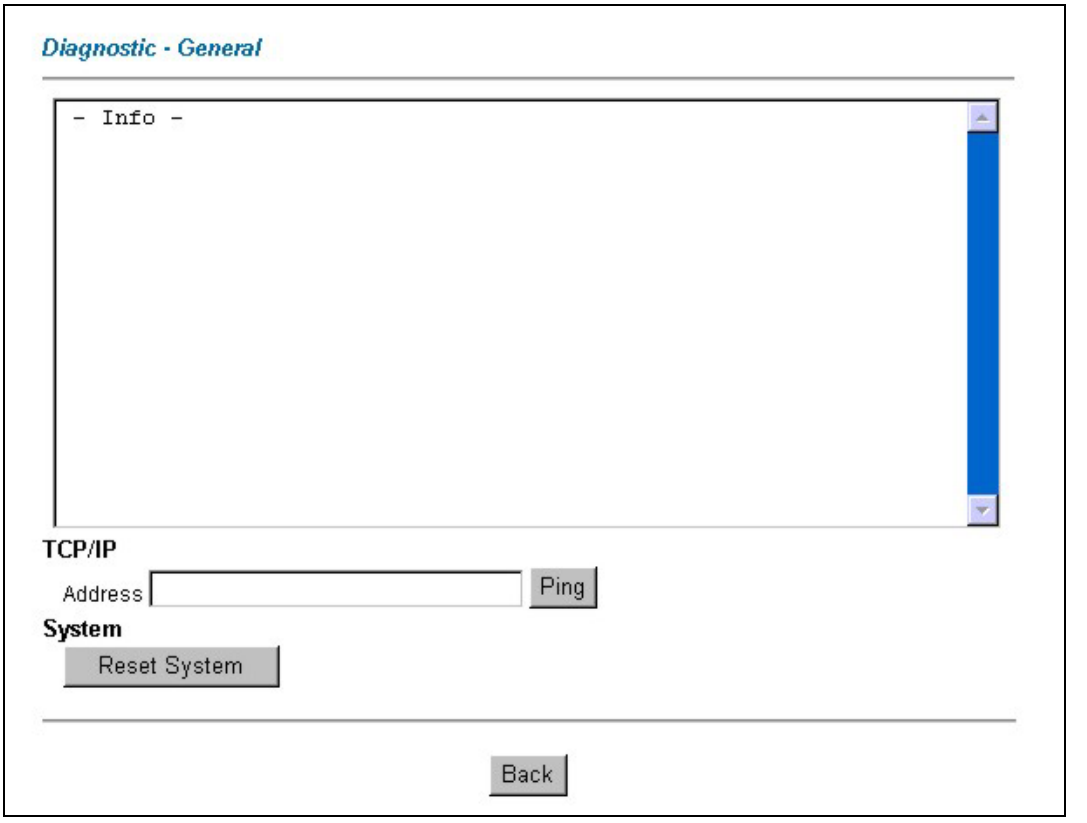


Figure 9-5 Diagnostic General

The following table describes the labels in this screen.

Table 9-4 Diagnostic General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection.
Ping	Click this button to ping the IP address that you entered.
Reset System	Click this button to reboot the Prestige. A warning dialog box is then displayed asking you if you're sure you want to reboot the system. Click **OK** to proceed.

Table 9-4 Diagnostic General

LABEL	DESCRIPTION
Back	Click this button to go back to the main **Diagnostic** screen.

9.4.2 Diagnostic DSL Line Screen

Click **Diagnostic** and then **DSL Line** to open the screen shown next.

Figure 9-6 Diagnostic DSL Line

The following table describes the labels in this screen.

Table 9-5 Diagnostic DSL Line

LABEL	DESCRIPTION
Reset ADSL Line	Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example: "Start to reset ADSL Loading ADSL modem F/W... Reset ADSL Line Successfully!"
ATM Status	Click this button to view ATM status.
ATM Loopback Test	Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The Prestige sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the Prestige. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.
Upstream Noise Margin	Click this button to display the upstream noise margin.
Downstream Noise Margin	Click this button to display the downstream noise margin.
Back	Click this button to go back to the main **Diagnostic** screen.

9.5 Firmware Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "Prestige.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See the *Firmware and Configuration File Maintenance* chapter in the parts that document the SMT for upgrading firmware using FTP/TFTP commands.

Only use firmware for your Prestige's specific model. Refer to the label on the bottom of your Prestige.

Click **Firmware** to open the following screen. Follow the instructions in this screen to upload firmware to your Prestige.

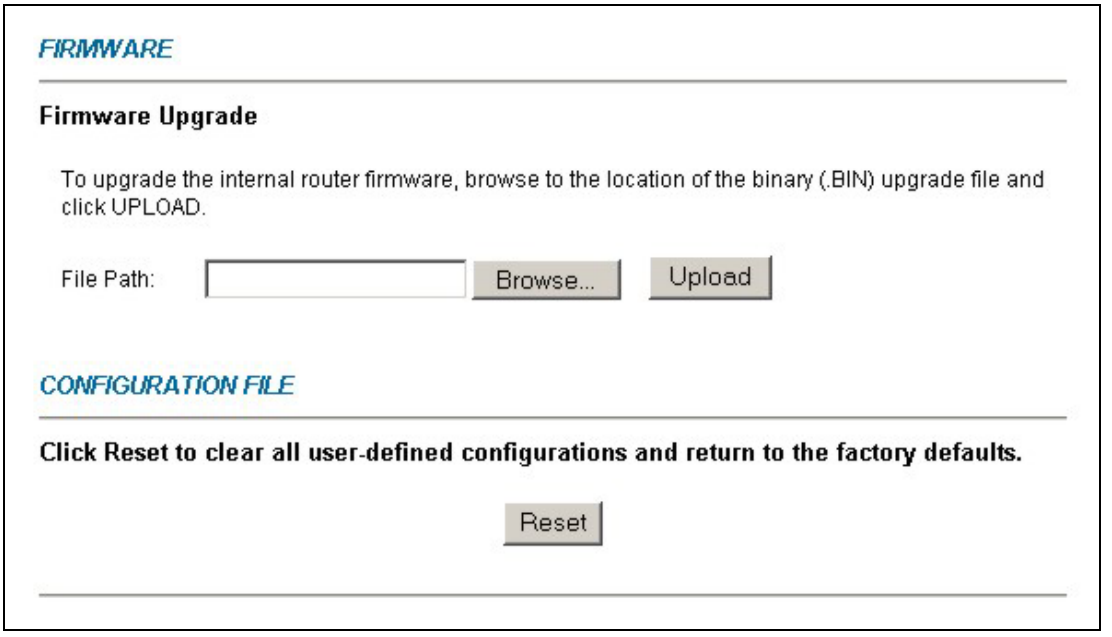

FIRMWARE
Firmware Upgrade
To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click UPLOAD.
File Path:
Browse...
Upload
CONFIGURATION FILE
Click Reset to clear all user-defined configurations and return to the factory defaults.
Reset

Figure 9-7 Firmware Upgrade

The following table describes the labels in this screen.

Table 9-6 Firmware Upgrade

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.
Reset	Click this button to clear all user-entered configuration information and return the Prestige to its factory defaults. Refer to the *Resetting the Prestige* section.

Do not turn off the Prestige while firmware upload is in progress!

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the Prestige again.

The Prestige automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 9-8 Network Temporarily Disconnected

After two minutes, log in again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the following screen will appear. Click **Back** to go back to the **Firmware** screen.

Figure 9-9 Error Message

Part VI:

SMT General Configuration

This part covers System Management Terminal configuration for general setup, Ethernet setup, Internet access, remote nodes, remote node TCP/IP, static routing and NAT.

See the web configurator parts of this guide for background information on features configurable by web configurator and SMT.

Chapter 10
Introducing the SMT

This chapter explains how to access and navigate the System Management Terminal and gives an overview of its menus.

10.1 SMT Introduction

The Prestige's SMT (System Management Terminal) is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection.

10.1.1 Procedure for SMT Configuration via Telnet

The following procedure details how to telnet into your Prestige.

Step 1. In Windows, click **Start** (usually in the bottom left corner), **Run** and then type "telnet 192.168.1.1" (the default IP address) and click **OK**.

Step 2. For your first login, enter the default password "1234". As you type the password, the screen displays an asterisk "*" for each character you type.

```
Password : xxxx
```

Figure 10-1 Login Screen

Step 3. After entering the password you will see the main menu.

Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your Prestige will automatically log you out. You will then have to telnet into the Prestige again.

10.1.2 Prestige SMT Menu Overview

The following figure gives you an overview of the various SMT menu screens of your Prestige.

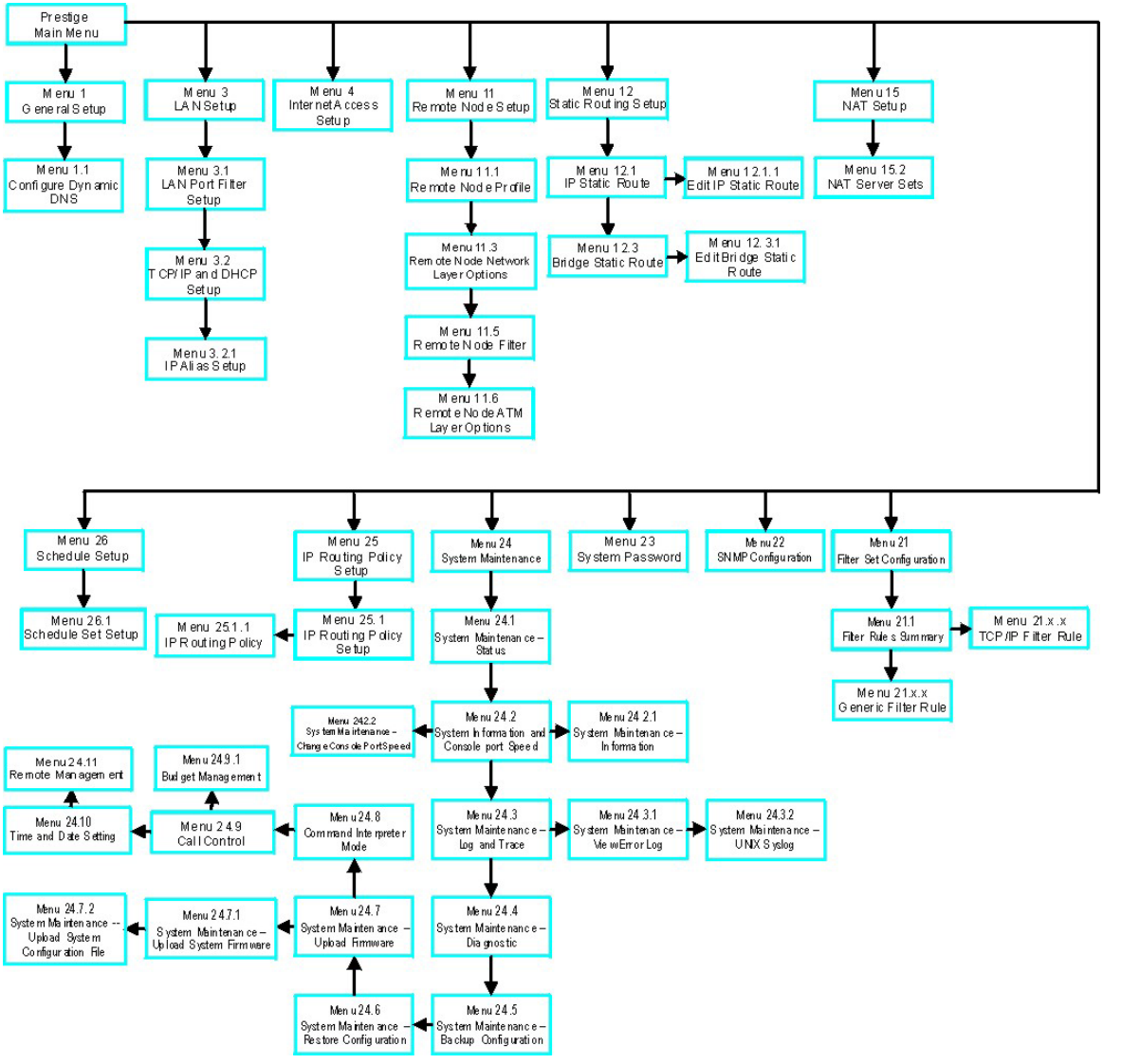

Prestige Main Menu
Menu 1 General Setup
Menu 1.1 Configure Dynamic DNS
Menu 3 LAN Setup
Menu 3.1 LAN Port Filter Setup
Menu 3.2 TCP/IP and DHCP Setup
Menu 3.2.1 IP Alias Setup
Menu 4 Internet Access Setup
Menu 11 Remote Node Setup
Menu 11.1 Remote Node Profile
Menu 11.3 Remote Node Network Layer Options
Menu 11.5 Remote Node Filter
Menu 11.6 Remote Node ATM Layer Options
Menu 12 Static Routing Setup
Menu 12.1 IP Static Route
Menu 12.1.1 Edit IP Static Route
Menu 12.3 Bridge Static Route
Menu 12.3.1 Edit Bridge Static Route
Menu 15 NAT Setup
Menu 15.2 NAT Server Sets
Menu 26 Schedule Setup
Menu 26.1 Schedule Set Setup
Menu 25 IP Routing Policy Setup
Menu 25.1 IP Routing Policy Setup
Menu 25.1.1 IP Routing Policy
Menu 24 System Maintenance
Menu 24.1 System Maintenance – Status
Menu 24.2 System Information and Console port Speed
Menu 24.2.1 System Maintenance – Information
Menu 24.2.2 System Maintenance – Change Console Port Speed
Menu 24.3 System Maintenance – Log and Trace
Menu 24.3.1 System Maintenance – View Error Log
Menu 24.3.2 System Maintenance – UNIX Syslog
Menu 24.4 System Maintenance – Diagnostic
Menu 24.5 System Maintenance – Backup Configuration
Menu 24.6 System Maintenance – Restore Configuration
Menu 24.7 System Maintenance – Upload Firmware
Menu 24.7.1 System Maintenance – Upload System Firmware
Menu 24.7.2 System Maintenance – Upload System Configuration File
Menu 24.8 Command Interpreter Mode
Menu 24.9 Call Control
Menu 24.9.1 Budget Management
Menu 24.10 Time and Date Setting
Menu 24.11 Remote Management
Menu 23 System Password
Menu 22 SNMP Configuration
Menu 21 Filter Set Configuration
Menu 21.1 Filter Rules Summary
Menu 21.x.x TCP/IP Filter Rule
Menu 21.x.x Generic Filter Rule

Figure 10-2 Prestige 623ME-T SMT Menu Overview

10.2 Navigating the SMT Interface

The SMT (System Management Terminal) is the interface that you use to configure your Prestige.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 10-1 Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.
Move to a "hidden" menu	Press [SPACE BAR] to change **No** to **Yes** then press [ENTER].	Fields beginning with "Edit" lead to hidden menus and have a default setting of **No**. Press [SPACE BAR] once to change **No** to **Yes**, then press [ENTER] to go to the "hidden" menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys.	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Entering information	Type in or press [SPACE BAR], then press [ENTER].	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<? > or **ChangeMe**	All fields with the symbol <?> must be filled in order to be able to save the new configuration. All fields with **ChangeMe** must not be left blank in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

After you enter the password, the SMT displays the main menu, as shown next.

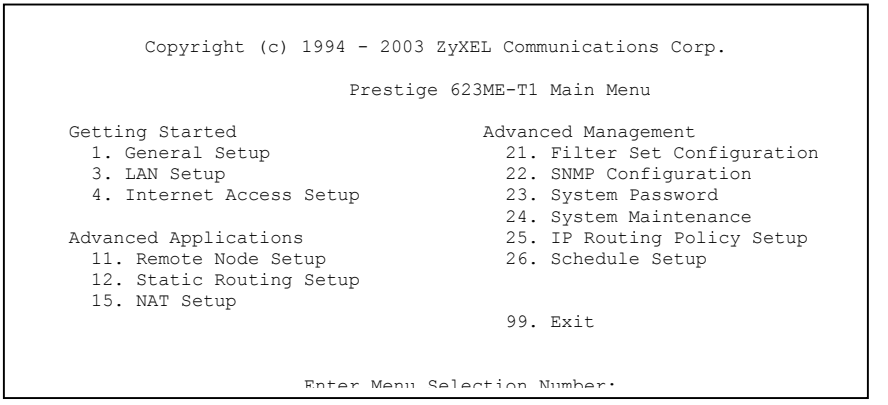


Figure 10-3 SMT Main Menu

10.2.1 System Management Terminal Interface Summary

Table 10-2 Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
3	LAN Setup	Use this menu to set up your LAN connection.
4	Internet Access Setup	A quick and easy way to set up an Internet connection.
11	Remote Node Setup	Use this menu to set up the Remote Node for LAN-to-LAN connection, including Internet connection.
12	Static Routing Setup	Use this menu to set up static routes.
15	NAT Setup	Use this menu to specify inside servers when NAT is enabled.
21	Filter Set Configuration	Use this menu to set up filters to provide security, etc.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Password	Use this menu to change your password.
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
25	IP Routing Policy Setup	Use this menu to configure your IP routing policy.
26	Schedule Setup	Use this menu to schedule outgoing calls.
99	Exit	Use this to exit from SMT and return to a blank screen.

10.3 Changing the System Password

Change the Prestige default password by following the steps shown next.

Step 1. Enter 23 in the main menu to display **Menu 23 - System Security** as shown next.

Step 2. Type your existing system password in the **Old Password** field, for example "1234", and press [ENTER].

```
                    Menu 23 - System Password

          Old Password= ?
          New Password= ?
          Retype to confirm= ?



           Enter here to CONFIRM or ESC to CANCEL:
```

Figure 10-4 Menu 23 System Password

Step 3. Type your new system password in the **New Password** field (up to 30 characters), and press [ENTER].

Step 4. Re-type your new system password in the **Retype to confirm** field for confirmation and press [ENTER].

Note that as you type a password, the screen displays an "*" for each character you type.

Chapter 11
General Setup

Menu 1 - General Setup contains administrative and system-related information.

11.1 General Setup

Menu 1 — General Setup contains administrative and system-related information (shown next). The **System Name** field is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the **Identification** tab, note the entry for the **Computer name** field and enter it as the Prestige **System Name**.
- In Windows 2000 click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the Prestige **System Name**.
- In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the Prestige **System Name**.

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the Prestige via DHCP.

11.2 Configuring Menu 1

Enter 1 in the Main Menu to open **Menu 1 — General Setup** (shown next).

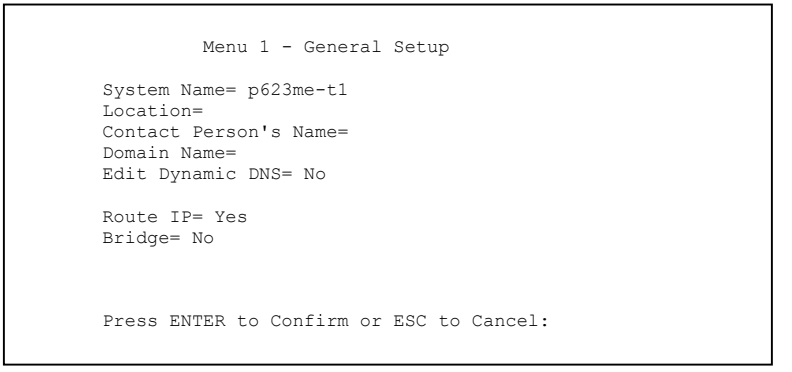


Figure 11-1 Menu 1 General Setup

Fill in the required fields. Refer to the table shown next for more information about these fields.

Table 11-1 Menu 1 General Setup

FIELD	DESCRIPTION	EXAMPLE
System Name	Enter a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.	P623ME-T1
Location (optional)	Enter the geographic location (up to 31 characters) of your Prestige.	MyHouse
Contact Person's Name (optional)	Enter the name (up to 30 characters) of the person in charge of this Prestige.	JohnDoe
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domainname" to see the current domain name used by your gateway. If you want to clear this field just press the [SPACE BAR]. The domain name entered by you is given priority over the ISP assigned domain name.	zyxel.com.tw
Edit Dynamic DNS	Press the [SPACE BAR] to select **Yes** or **No** (default). Select **Yes** to configure **Menu 1.1 — Configure Dynamic DNS** (discussed next).	**No**
Route IP	Set this field to **Yes** to enable or **No** to disable IP routing. You must enable IP routing for Internet access.	**Yes**
Bridge	Turn on/off bridging for protocols not supported (for example, SNA) or not turned on in the previous **Route IP** field. Select **Yes** to turn bridging on; select **No** to turn bridging off.	**No**

Table 11-1 Menu 1 General Setup

FIELD	DESCRIPTION	EXAMPLE
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

11.2.1 Configuring Dynamic DNS

If you have a private WAN IP address, then you cannot use Dynamic DNS.

To configure Dynamic DNS, go to **Menu 1 — General Setup** and select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1— Configure Dynamic DNS** as shown next.

```
                    Menu 1.1 - Configure Dynamic DNS

Service Provider= WWW.DynDNS.ORG
Active= No
Host=
EMAIL=
USER=
Password= ********
Enable Wildcard= No



                Press ENTER to Confirm or ESC to Cancel:
```

Figure 11-2 Menu 1.1 Configure Dynamic DNS

Follow the instructions in the next table to configure Dynamic DNS parameters.

Table 11-2 Menu 1.1 Configure Dynamic DNS

FIELD	DESCRIPTION	EXAMPLE
Service Provider	This is the name of your Dynamic DNS service provider.	WWW.DynDNS.ORG (default)
Active	Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active.	**Yes**
Host	Enter the domain name assigned to your Prestige by your Dynamic DNS provider.	me.dyndns.org
EMAIL	Enter your e-mail address.	mail@mailserver
USER	Enter your user name.	

Table 11-2 Menu 1.1 Configure Dynamic DNS

FIELD	DESCRIPTION	EXAMPLE
Password	Enter the password assigned to you.	
Enable Wildcard	Your Prestige supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** This field is **N/A** when you choose DDNS client as your service provider.	**No**
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

Chapter 12
LAN Setup

This chapter covers how to configure your wired Local Area Network (LAN) settings.

12.1 LAN Setup

This section describes how to configure the Ethernet using **Menu 3 — LAN Setup**. From the main menu, enter 3 to display menu 3.

```
                    Menu 3 - LAN Setup

          1. LAN Port Filter Setup
          2. TCP/IP and DHCP Setup




                Enter Menu Selection Number:
```

Figure 12-1 Menu 3 Ethernet Setup

12.1.1 LAN Port Filter Setup

This menu allows you to specify filter set(s) that you wish to apply to the Ethernet traffic. You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches.

```
                Menu 3.1 - LAN Port Filter Setup

          Input Filter Sets:
            protocol filters=
            device filters=
          Output Filter Sets:
            protocol filters=
            device filters=

          Press ENTER to Confirm or ESC to Cancel:
```

Figure 12-2 Menu 3.1 LAN Port Filter Setup

If you need to define filters, please read the *Filter Set Configuration* chapter first, then return to this menu to define the filter sets.

12.2 Protocol Dependent Ethernet Setup

Depending on the protocols for your applications, you need to configure the respective Ethernet Setup, as outlined below.

- For TCP/IP Ethernet setup refer to the *Internet Access Application* chapter.
- For bridging Ethernet setup refer to the *Bridging Setup* chapter.

12.3 TCP/IP Ethernet Setup and DHCP

Use menu 3.2 to configure your Prestige for TCP/IP.

To edit menu 3.2, enter 3 from the main menu to display **Menu 3 — Ethernet Setup**. When menu 3 appears, press 2 and press [ENTER] to display **Menu 3.2 — TCP/IP and DHCP Ethernet Setup**, as shown next:

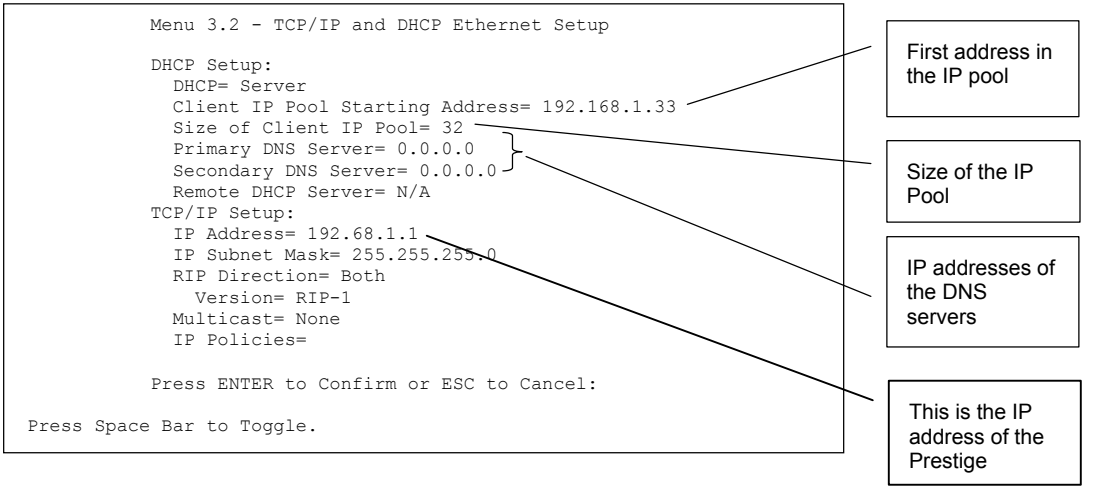

Menu 3.2 - TCP/IP and DHCP Ethernet Setup
DHCP Setup:
DHCP= Server
Client IP Pool Starting Address= 192.168.1.33
Size of Client IP Pool= 32
Primary DNS Server= 0.0.0.0
Secondary DNS Server= 0.0.0.0
Remote DHCP Server= N/A
TCP/IP Setup:
IP Address= 192.68.1.1
IP Subnet Mask= 255.255.255.0
RIP Direction= Both
Version= RIP-1
Multicast= None
IP Policies=
Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
First address in the IP pool
Size of the IP Pool
IP addresses of the DNS servers
This is the IP address of the Prestige

Figure 12-3 Menu 3.2 TCP/IP and DHCP Ethernet Setup

Follow the instructions in the following table on how to configure the DHCP fields.

Table 12-1 DHCP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
DHCP Setup		
DHCP	If set to **Server**, your Prestige can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to **None**, the DHCP server will be disabled. If set to **Relay**, the Prestige acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server in this case. When DHCP is used, the following items need to be set:	**Server** (default)
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size or count of the IP address pool.	32
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	
Remote DHCP Server	If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here.	

Follow the instructions in the following table to configure TCP/IP parameters for the Ethernet port.

Table 12-2 TCP/IP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
TCP/IP Setup		
IP Address	Enter the (LAN) IP address of your Prestige in dotted decimal notation	192.168.1.1
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige.	255.255.255.0
RIP Direction	Press [SPACE BAR] to select the RIP direction. Choices are **Both**, **In Only**, **Out Only** or **None**.	**Both** (default)
Version	Press [SPACE BAR] to select the RIP version. Choices are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1** (default)

Table 12-2 TCP/IP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The Prestige supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** to disable it.	**None** (default)
IP Policies	Create policies using SMT menu 25 (see the *IP Policy Routing chapter*) and apply them on the Prestige LAN interface here. You can apply up to four IP Policy sets (from twelve) by entering their numbers separated by commas.	2,4,7,9

Chapter 13
Internet Access

This chapter shows you how to configure the LAN and WAN of your Prestige for Internet access.

13.1 Internet Access Overview

Refer to the chapters on the web configurator's wizard, LAN and WAN screens for more background information on fields in the SMT screens covered in this chapter.

13.2 IP Policies

Traditionally, routing is based on the destination address *only* and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing. Create policies using SMT menu 25 (see *IP Policy Routing*) and apply them on the Prestige LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN).

13.3 Route IP Setup

The first step is to enable the IP routing in **Menu 1 — General Setup**.

To edit menu 1, type in 1 in the main menu and press [ENTER]. Set the **Route IP** field to **Yes** by pressing [SPACE BAR].

```
                Menu 1 - General Setup

System Name= P623ME-T1
Location= location
Contact Person's Name=
Domain Name=
Edit Dynamic DNS= No

Route IP= Yes
Bridge= No

Press ENTER to Confirm or ESC to Cancel:
```

Figure 13-1 Menu 1 General Setup

13.4 Internet Access Configuration

Menu 4 allows you to enter the Internet Access information in one screen. Menu 4 is actually a simplified setup for one of the remote nodes that you can access in menu 11. Before you configure your Prestige for Internet access, you need to collect your Internet account information.

Use the *Internet Access Checklist* table in the *Read Me First* to record your Internet account information. Note that if you are using PPPoA or PPPoE encapsulation, then the only ISP information you need is a login name and password. You only need to know the Ethernet Encapsulation Gateway IP address if you are using ENET ENCAP encapsulation.

From the main menu, type 4 to display **Menu 4 - Internet Access Setup**, as shown next.

```
                Menu 4 - Internet Access Setup

        ISP's Name= MyISP
        Encapsulation= PPPoE
        Multiplexing= LLC-based
        VPI #= 1
        VCI #= 32
        ATM QoS Type= CBR
          Peak Cell Rate (PCR)= 0
          Sustain Cell Rate (SCR)= 0
          Maximum Burst Size (MBS)= 0
        My Login= N/A
        My Password= N/A
        ENET ENCAP Gateway= 0.0.0.0
        IP Address Assignment= Static
          IP Address= 0.0.0.0
        Network Address Translation= SUA Only
          Address Mapping Set= N/A

        Press ENTER to Confirm or ESC to Cancel:
```

Figure 13-2 Menu 4 Internet Access Setup

The following table contains instructions on how to configure your Prestige for Internet access.

Table 13-1 Menu 4 Internet Access Setup

FIELD	DESCRIPTION	EXAMPLE
ISP's Name	Enter the name of your Internet Service Provider. This information is for identification purposes only.	MyISP
Encapsulation	Press [SPACE BAR] to select the method of encapsulation used by your ISP. Choices are **PPPoE** and **RFC 1483**.	PPPoE

Table 13-1 Menu 4 Internet Access Setup

FIELD	DESCRIPTION	EXAMPLE
Multiplexing	Press [SPACE BAR] to select the method of multiplexing used by your ISP. Choices are **VC-based** or **LLC-based**.	LLC-based
VPI #	Enter the Virtual Path Identifier (VPI) assigned to you.	8
VCI #	Enter the Virtual Channel Identifier (VCI) assigned to you.	35
ATM QoS Type	Press [SPACE BAR] and select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR** (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.	UBR
Peak Cell Rate (PCR)	This is the maximum rate at which the sender can send cells. Type the PCR.	0
Sustain Cell Rate (SCR)	Sustained Cell Rate is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-type traffic. Type the SCR; it must be less than the PCR.	0
Maximum Burst Size (MBS)	Refers to the maximum number of cells that can be sent at the peak rate. Type the MBS. The MBS must be less than 65535.	0
My Login	Configure the **My Login** and **My Password** fields for PPPoA and PPPoE encapsulation only. Enter the login name that your ISP gives you. If you are using PPPoE encapsulation**,** then this field must be of the form user@domain where domain identifies your PPPoE service name.	N/A
My Password	Enter the password associated with the login name above.	N/A
Idle Timeout	This value specifies the number of idle seconds that elapse before the Prestige automatically disconnects the PPPoE session.	0
IP Address Assignment	Press [SPACE BAR] to select **Static** or **Dynamic** address assignment.	Dynamic
IP Address	Enter the IP address supplied by your ISP if applicable.	N/A
Network Address Translation	Press [SPACE BAR] to select **None**, **SUA Only** or **Full Feature**. Please see the *NAT Chapter* for more details on the SUA (Single User Account) feature.	**SUA Only**

Table 13-1 Menu 4 Internet Access Setup

FIELD	DESCRIPTION	EXAMPLE
Address Mapping Set	When **Full Feature** is selected in the **NAT** field, configure address mapping sets in menu 15.1. Type the numbers of mapping sets (1-8) to use with NAT. See the *NAT* chapter for details. When **SUA Only** is selected in the **NAT** field, the SMT uses NAT server set 1 in menu 15.1 (see the *NAT* chapter for details).	**N/A**
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

If all your settings are correct your Prestige should connect automatically to the Internet. If the connection fails, note the error message that you receive on the screen and take the appropriate troubleshooting steps.

Chapter 14
Remote Node Configuration

This chapter covers remote node configuration.

14.1 Remote Node Setup Overview

This section describes the protocol-independent parameters for a remote node. A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. When you use menu 4 to set up Internet access, you are configuring one of the remote nodes.

You first choose a remote node in **Menu 11- Remote Node Setup**. You can then edit that node's profile in menu 11.1, as well as configure specific settings in three submenus: edit IP and bridge options in menu 11.3; edit ATM options in menu 11.6; and edit filter sets in menu 11.5.

14.2 Remote Node Setup

This section describes the protocol-independent parameters for a remote node.

14.2.1 Remote Node Profile

To configure a remote node, follow these steps:

Step 1. From the main menu, enter 11 to display **Menu 11 - Remote Node Setup.**

Step 2. When menu 11 appears, as shown in the following figure, type the number of the remote node that you want to configure.

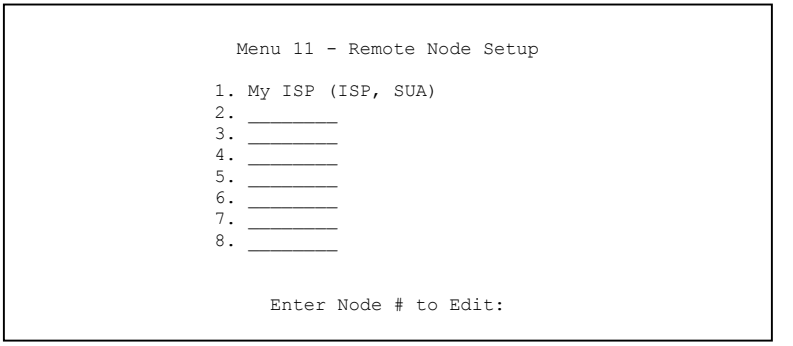


Figure 14-1 Menu 11 Remote Node Setup

14.2.2 Encapsulation and Multiplexing Scenarios

For Internet access you should use the encapsulation and multiplexing methods used by your ISP. Consult your ISP for information on encapsulation and multiplexing methods for LAN-to-LAN applications, for example between a branch office and corporate headquarters. There must be prior agreement on encapsulation and multiplexing methods because they cannot be automatically determined. What method(s) you use also depends on how many VCs you have and how many different network protocols you need. The extra overhead that ENET ENCAP encapsulation entails makes it a poor choice in a LAN-to-LAN application.

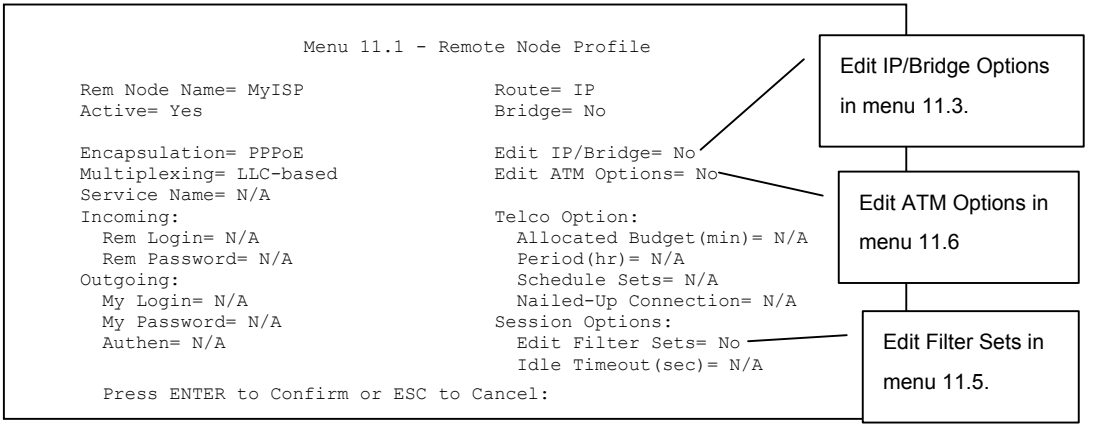


Figure 14-2 Menu 11.1 Remote Node Profile

In **Menu 11.1 – Remote Node Profile**, fill in the fields as described in the following table.

Table 14-1 Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Type a unique, descriptive name of up to eight characters for this node.	MyISP
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate or **No** to deactivate this node. Inactive nodes are displayed with a minus sign "–" in SMT menu 11.	**Yes**
Encapsulation	Select the encapsulation type your ISP uses **PPPoE** - A dial up connection that uses PPPoE encapsulation and requires a username and password. **RFC 1483** - An always up connection that uses the RFC1483 protocol.	**PPPoE**
Multiplexing	Press [SPACE BAR] and then [ENTER] to select the method of multiplexing that your ISP uses, either **VC-based** or **LLC-based**.	**LLC-based**
Service Name	When using **PPPoE** encapsulation, type the name of your PPPoE service here.	N/A
Incoming:		

Table 14-1 Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Rem Login	Type the login name that this remote node will use to call your Prestige. The login name and the **Rem Password** will be used to authenticate this node.	
Rem Password	Type the password used when this remote node calls your Prestige.	
Outgoing:		
My Login	Type the login name assigned by your ISP when the Prestige calls this remote node.	
My Password	Type the password assigned by your ISP when the Prestige calls this remote node.	
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP**/**PAP** – Your Prestige will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** – accept **CHAP** (Challenge Handshake Authentication Protocol) only. **PAP** – accept PAP (Password Authentication Protocol) only.	
Route	This field determines the protocol used in routing. Options are **IP** and **None.**	**IP**
Bridge	When bridging is enabled, your Prestige will forward any packet that it does not route to this remote node; otherwise, the packets are discarded. Select **Yes** to enable and **No** to disable.	**No**
Edit IP/Bridge	Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options**.	**No**
Edit ATM Options	Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 11.6 – Remote Node ATM Layer Options**.	**No**
Telco Option		
Allocated Budget (min)	This sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.	
Period (hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the **Allocated Budget** is (10 minutes) and the **Period (hr)** is 1 (hour).	

Table 14-1 Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Schedule Sets	This field is only applicable for **PPPoE** and **PPPoA** encapsulation. You can apply up to four schedule sets here. For more details please refer to the *Call Scheduling* chapter.	
Nailed up Connection	This field is only applicable for **PPPoE** encapsulation. This field specifies if you want to make the connection to this remote node a nailed-up connection.	
Session Options		
Edit Filter Sets	Use [SPACE BAR] to choose **Yes** and press [ENTER] to open menu 11.5 to edit the filter sets. See the *Remote Node Filter* section for more details.	**No** (default)
Idle Timeout (sec)	Type the number of seconds (0-9999) that can elapse when the Prestige is idle (there is no traffic going to the remote node), before the Prestige automatically disconnects the remote node. 0 means that the session will not timeout.	
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

14.2.3 Outgoing Authentication Protocol

For obvious reasons, you should employ the strongest authentication protocol possible. However, some vendors' implementation includes specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If the peer disconnects right after a successful authentication, make sure that you specify the correct authentication protocol when connecting to such an implementation.

14.3 Metric

The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

The metric sets the priority for the Prestige's routes to the Internet. If any two of the default routes have the same metric, the Prestige uses the following pre-defined priorities:

1. Normal route: designated by the ISP
2. Traffic-redirect route

IP Policy Routing overrides the default routing behavior and takes priority over all of the routes mentioned above (see the *IP Policy Routing* chapter).

For example, if the normal route has a metric of "1" and the traffic-redirect route has a metric of "2", then the normal route acts as the primary default route. If the normal route fails to connect to the Internet, the Prestige tries the traffic-redirect route next.

14.4 Remote Node Network Layer Options

For the TCP/IP parameters, perform the following steps to edit **Menu 11.3 – Remote Node Network Layer Options** as shown next.

Step 1. In menu 11.1, make sure **IP** is among the protocols in the **Route** field.

Step 2. Move the cursor to the **Edit IP/Bridge** field, press [SPACE BAR] to select **Yes,** then press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options.**

```
               Menu 11.3 - Remote Node Network Layer Options

   IP Options:                          Bridge Options:
      IP Address Assignment= Dynamic      Ethernet Addr Timeout (min)= N/A
      Rem IP Addr: 0.0.0.0
      Rem Subnet Mask= 0.0.0.0
      My WAN Addr= 0.0.0.0
      NAT= Full Feature
        Address Mapping Set= 2
      Metric= 2
      Private= No
      RIP Direction= None
         Version= RIP-1
      Multicast= None
      IP Policies= 3,4,5,6

Press ENTER to Confirm or ESC to Cancel:
```

Figure 14-3 Menu 11.3 Remote Node Network Layer Options

The next table explains fields in **Menu 11.3 – Remote Node Network Layer Options**.

Table 14-2 Menu 11.3 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select **Dynamic** if the remote node is using a dynamically assigned IP address or **Static** if it is using a static (fixed) IP address. You will only be able to configure this in the ISP node (also the one you configure in menu 4). All other nodes are set to **Static**.	**Dynamic**
Rem IP Addr	This is the IP address you entered in the previous menu.	
Rem Subnet Mask	Type the subnet mask assigned to the remote node.	
My WAN Addr	Some implementations, especially UNIX derivatives, require separate IP network numbers for the WAN and LAN links and each end to have a unique address within the WAN network number. In that case, type the IP address assigned to the WAN port of your Prestige. **Refers to local Prestige address, not the remote router address.**	
NAT	Press [SPACE BAR] and then [ENTER] to select **Full Feature** if you have multiple public WAN IP addresses for your Prestige. Select **SUA Only** if you have just one public WAN IP address for your Prestige. The SMT uses Address Mapping Set 255 (menu 15.1 - see section ***Error! Reference source not found.***). Select **None** to disable NAT.	**SUA Only**
Address Mapping Set	When **SUA Only** is selected in the **NAT** field, the SMT uses NAT server set 1 in menu 15.2 (see the *NAT* chapter for details).	1
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the cost measurement, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	2
Private	This determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.	**No**
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP Direction. Options are **Both**, **In Only**, **Out Only** or **None**.	**None**

Table 14-2 Menu 11.3 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1**
Multicast	**IGMP-v1** sets IGMP to version 1, **IGMP-v2** sets IGMP to version 2 and **None** disables IGMP.	**None**
IP Policies	You can apply up to four IP Policy sets (from 12) by typing in their numbers separated by commas. Configure the filter sets in menu 25 first (see the *IP Policy Routing* chapter) and then apply them here.	3, 4, 5, 6
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

14.4.1 My WAN Addr Sample IP Addresses

The following figure uses sample IP addresses to help you understand the field of **My WAN Addr** in menu 11.3. Refer to the previous *LAN and WAN IP Addresses* figure in the web configurator chapter on LAN setup for a brief review of what a WAN IP is. **My WAN Addr** indicates the local Prestige WAN IP (172.16.0.1 in the following figure) while **Rem IP Addr** indicates the peer WAN IP (172.16.0.2 in the following figure).

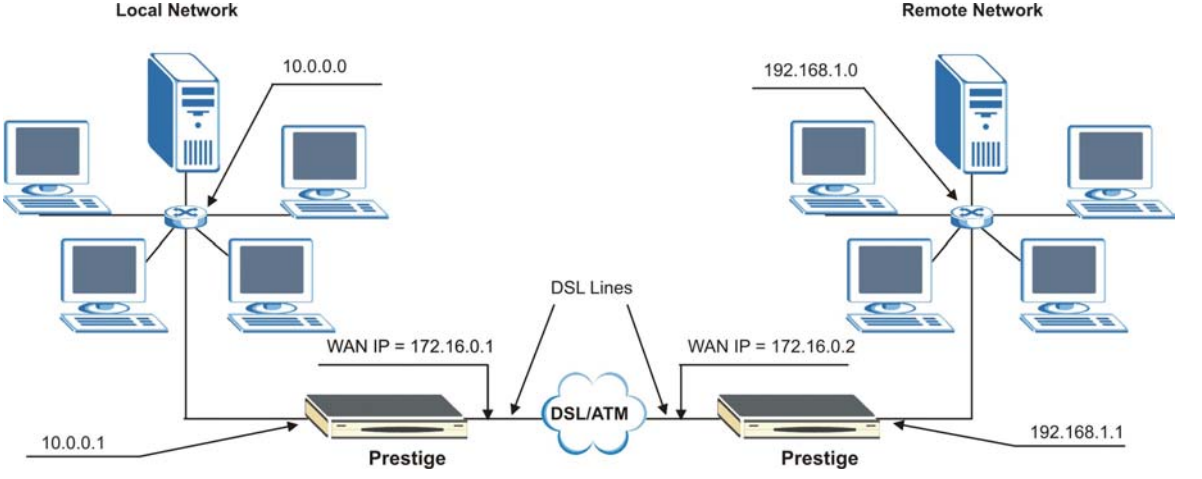


Figure 14-4 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection

14.5 Remote Node Filter

Move the cursor to the **Edit Filter Sets** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to display **Menu 11.5 – Remote Node Filter**.

Use **Menu 11.5 – Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige and also to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by comma, for example, 1, 5, 9, 12, in each filter field.

Note that spaces are accepted in this field. The Prestige has a prepackaged filter set, NetBIOS_WAN, that blocks NetBIOS packets (call protocol filter = 1). Include this in the call filter sets if you want to prevent NetBIOS packets from triggering calls to a remote node.

```
                Menu 11.5 - Remote Node Filter

                     Input Filter Sets:
                       protocol filters= 11, 12
                         device filters=
                     Output Filter Sets:
                       protocol filters=
                         device filters=

          Enter here to CONFIRM or ESC to CANCEL:
```

Figure 14-5 Menu 11.5 Remote Node Filter (RFC 1483 Encapsulation)

```
                Menu 11.5 - Remote Node Filter

                     Input Filter Sets:
                       protocol filters= 11, 12
                         device filters=
                     Output Filter Sets:
                       protocol filters=
                         device filters=
                       Call Filter Sets:
                       Protocol filters=
                         Device filters=

          Enter here to CONFIRM or ESC to CANCEL:
```

Figure 14-6 Menu 11.5 Remote Node Filter (PPPoE Encapsulation)

14.5.1 Web Configurator Internet Security Filter Rules

In the web configurator, open the **Security** screen as shown next. Select the predefined filter rules and click **Apply**.

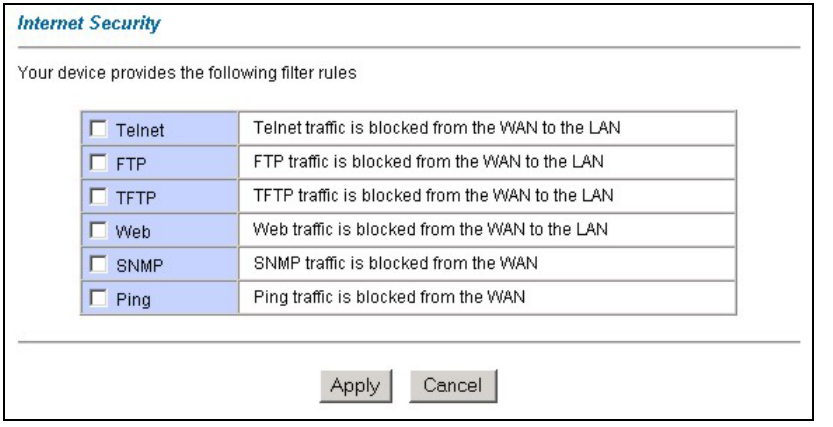

Internet Security
Your device provides the following filter rules
Telnet
Telnet traffic is blocked from the WAN to the LAN
FTP
FTP traffic is blocked from the WAN to the LAN
TFTP
TFTP traffic is blocked from the WAN to the LAN
Web
Web traffic is blocked from the WAN to the LAN
SNMP
SNMP traffic is blocked from the WAN
Ping
Ping traffic is blocked from the WAN
Apply
Cancel

Figure 14-7 Internet Security

Once you apply the filter rules in the web configurator, filter sets 11 and 12 are automatically applied in the **protocol filters** field under **Input Filter Sets** in SMT menu 11.5.

SMT input protocol filter set numbers that were previously applied are erased after you apply the Internet Security **filter rules in the web configurator. To reapply them or apply new filter sets, you need to enter the filter set numbers again along with filter sets 11 and 12. For example, to apply filter sets 1 and 2, you enter "1, 2, 11, 12".**

14.5.2 Web Configurator Filter Sets

When you apply filter rules using the web configurator, filter sets 11 and 12 are automatically generated in SMT menu 21.

```
                    Menu 21 - Filter Set Configuration

Filter                                  Filter
Set #        Comments                   Set #        Comments
------  -----------------               ------  -----------------
  1      NetBIOS_WAN                      7      _________________
  2      NetBIOS_LAN                      8      _________________
  3      PPPoE                            9      _________________
  4                                      10      _________________
  5                                      11      WebSet1
  6      _________________               12      WebSet2


                Enter Filter Set Number to Configure= 0
                Edit Comments= N/A
                Press ENTER to Confirm or ESC to Cancel:
```

Figure 14-8 Menu 21- Filer Set Configuration

The following figures display the filter rules in filter sets 11 and 12.

```
                    Menu 21.11 - Filter Rules Summary
# A Type                        Filter Rules                          M m n
- - ---- ------------------------------------------------------------ - - -
1 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=161                        N D N
2 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=162                        N D F
3 N
4 N
5 N
6 N

               Enter Filter Rule Number (1-6) to Configure:
```

Figure 14-9 Menu 21.11- WebSet 11

```
                    Menu 21.12 - Filter Rules Summary

# A Type                        Filter Rules                          M m n
- - ---- ------------------------------------------------------------ - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23                          N D N
2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21                          N D N
3 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=69                         N D N
4 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=80                          N D N
5 Y IP   Pr=1, SA=0.0.0.0, DA=0.0.0.0, DP=0                           N D N
6 N

               Enter Filter Rule Number (1-6) to Configure
```

Figure 14-10 Menu 21.12- WebSet 12

Do not edit filter sets 11 and 12. They are used exclusively by the web configurator. Any rules you configured in sets 11 and 12 will be erased and replaced when you apply the web configurator-generated filter rules.

14.6 Editing ATM Layer Options

Follow the steps shown next to edit **Menu 11.6 – Remote Node ATM Layer Options**.

In menu 11.1, move the cursor to the **Edit ATM Options** field and then press [SPACE BAR] to select **Yes**. Press [ENTER] to display **Menu 11.6 – Remote Node ATM Layer Options**.

There are two versions of menu 11.6 for the Prestige, depending on whether you chose **VC-based**/**LLC-based** multiplexing and **PPP** encapsulation in menu 11.1.

14.6.1 VC-based Multiplexing (non-PPP Encapsulation)

For **VC-based** multiplexing, by prior agreement, a protocol is assigned a specific virtual circuit, for example, VC1 will carry IP. Separate VPI and VCI numbers must be specified for each protocol.

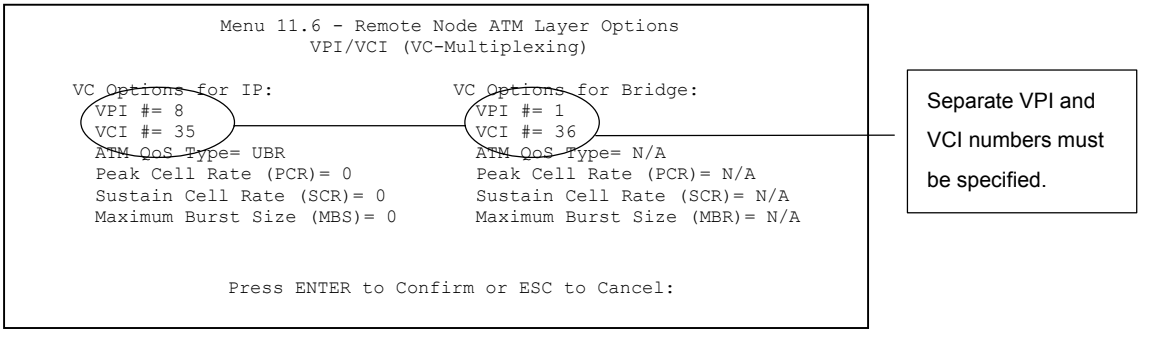

Menu 11.6 - Remote Node ATM Layer Options
VPI/VCI (VC-Multiplexing)
VC Options for IP:
VPI #= 8
VCI #= 35
ATM QoS Type= UBR
Peak Cell Rate (PCR)= 0
Sustain Cell Rate (SCR)= 0
Maximum Burst Size (MBS)= 0
VC Options for Bridge:
VPI #= 1
VCI #= 36
ATM QoS Type= N/A
Peak Cell Rate (PCR)= N/A
Sustain Cell Rate (SCR)= N/A
Maximum Burst Size (MBR)= N/A
Press ENTER to Confirm or ESC to Cancel:
Separate VPI and VCI numbers must be specified.

Figure 14-11 Menu 11.6 for VC-based Multiplexing

14.6.2 LLC-based Multiplexing or PPP Encapsulation

For **LLC-based** multiplexing or **PPP** encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header.

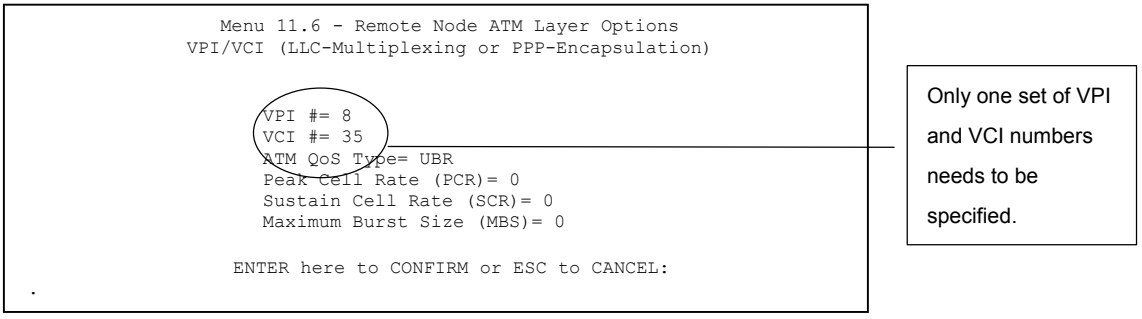

Menu 11.6 - Remote Node ATM Layer Options
VPI/VCI (LLC-Multiplexing or PPP-Encapsulation)
VPI #= 8
VCI #= 35
ATM QoS Type= UBR
Peak Cell Rate (PCR)= 0
Sustain Cell Rate (SCR)= 0
Maximum Burst Size (MBS)= 0
ENTER here to CONFIRM or ESC to CANCEL:
Only one set of VPI and VCI numbers needs to be specified.

Figure 14-12 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation

In this case, only one set of VPI and VCI numbers need be specified for all protocols. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (1 to 31 is reserved for local management of ATM traffic).

Chapter 15
Static Route Setup

This chapter shows how to setup IP static routes.

15.1 IP Static Route Overview

Static routes tell the Prestige routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node.

Each remote node specifies only the network to which the gateway is directly connected and the Prestige has no knowledge of the networks beyond. For instance, the Prestige knows about network N2 in the following figure through remote node Router 1. However, the Prestige is unable to route a packet to network N3 because it does not know that there is a route through remote node Router 1 (via Router 2). The static routes allow you to tell the Prestige about the networks beyond the remote nodes.

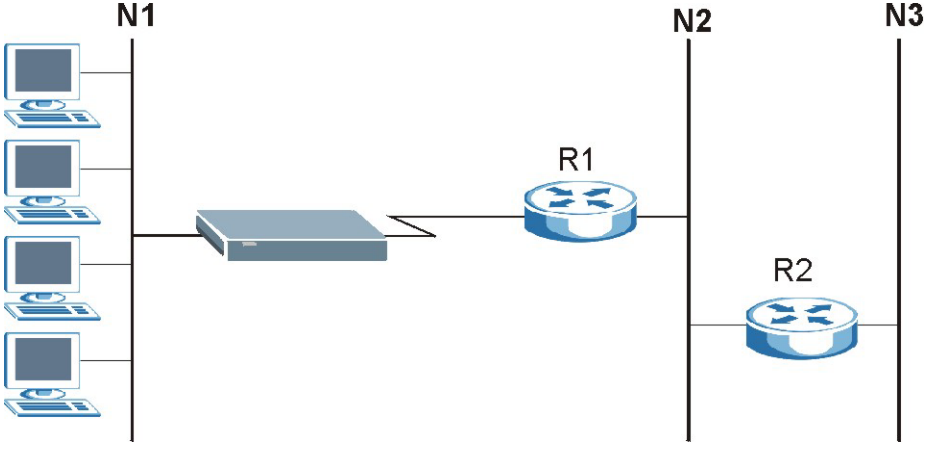


Figure 15-1 Sample Static Routing Topology

15.2 Configuring an IP static route

Step 1. To configure an IP static route, use **Menu 12 – Static Route Setup** (shown next).

```
Menu 12 - Static Route Setup

        1. IP Static Route
        3. Bridge Static Route


 Please enter selection:
```

Figure 15-2 Menu 12 Static Route Setup

Step 2. From menu 12, select 1 to open **Menu 12.1 — IP Static Route Setup** (shown next).

```
    Menu 12.1 - IP Static Route Setup

1. ________
2. ________
3. ________
4. ________
5. ________
6. ________
7. ________
8. ________
9. ________
10. ________
11. ________
12. ________
13. ________
14. ________
15. ________
16. ________
      Enter selection number:
```

Figure 15-3 Menu 12.1 IP Static Route Setup

Step 3. Now, type the route number of a static route you want to configure.

```
                Menu 12.1.1 - Edit IP Static Route

                   Route #: 1
                   Route Name= ?
                   Active= No
                   Destination IP Address= ?
                   IP Subnet Mask= ?
                   Gateway IP Address= ?
                   Metric= 2
                   Private= No

             Press ENTER to Confirm or ESC to Cancel:
```

Figure 15-4 Menu12.1.1 Edit IP Static Route

The following table describes the fields for **Menu 12.1.1 – Edit IP Static Route Setup**.

Table 15-1 Menu12.1.1 Edit IP Static Route

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.1.
Route Name	Type a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Type the subnet mask for this destination. Follow the discussion on *IP Subnet Mask* in this manual.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.

Table 15-1 Menu12.1.1 Edit IP Static Route

FIELD	DESCRIPTION
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and is not included in RIP broadcasts. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Chapter 16
Bridging Setup

This chapter shows you how to configure the bridging parameters of your Prestige.

16.1 Bridging Overview

Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware address, while routing does it on the network layer (IP) address. Bridging allows the Prestige to transport packets of network layer protocols that it does not route, for example, SNA, from one network to another. The caveat is that, compared to routing, bridging generates more traffic for the same network layer protocol, and it also demands more CPU cycles and memory.

For efficiency reasons, do *not* turn on bridging unless you need to support protocols other than IP on your network. For IP, enable the routing if you need it; do not bridge what the Prestige can route.

16.2 Bridge Ethernet Setup

Basically, all non-local packets are bridged to the WAN. Your Prestige does not support IPX.

16.2.1 Remote Node Bridging Setup

Follow the procedure in another section to configure the protocol-independent parameters in **Menu 11.1 – Remote Node Profile**. For bridging-related parameters, you need to configure **Menu 11.3 – Remote Node Network Layer Options**.

To setup **Menu 11.3 – Remote Node Network Layer Options** shown in the next figure, follow these steps:

Step 1. In menu 11.1, make sure the **Bridge** field is set to **Yes**.

```
                    Menu 11.1 - Remote Node Profile

  Rem Node Name= ?                      Route= IP
  Active= Yes                           Bridge= Yes

  Encapsulation= ENET ENCAP             Edit IP/Bridge= Yes
  Multiplexing= VC-based                Edit ATM Options= No
  Service Name= N/A
  Incoming:                             Telco Option:
    Rem Login= N/A                        Allocated Budget(min)= N/A
    Rem Password= N/A                     Period(hr)= N/A
  Outgoing:                               Schedule Sets= N/A
    My Login= N/A                         Nailed-Up Connection= N/A
    My Password= N/A                    Session Options:
    Authen= N/A                           Edit Filter Sets= No
                                          Idle Timeout(sec)= N/A


                Press ENTER to Confirm or ESC to Cancel:
```

Figure 16-1 Menu 11.1 Remote Node Profile

Step 2. Move the cursor to the **Edit IP/Bridge** field, then press [SPACE BAR] to set the value to **Yes** and press [ENTER] to edit **Menu 11.3 – Remote Node Network Layer Options**.

```
            Menu 11.3 - Remote Node Network Layer Options

    IP Options:                         Bridge Options:
     IP Address Assignment= Static      Ethernet Addr Timeout (min)= 0
     Rem IP Addr: 0.0.0.0
       Rem Subnet Mask= 0.0.0.0
       My WAN Addr= 0.0.0.0
       NAT= Full Feature
         Address Mapping Set=2
       Metric= 2
       Private= No
       RIP Direction= Both
         Version= RIP-2B
       Multicast= IGMP-v2
       IP Policies=

  Press ENTER to Confirm or ESC to Cancel:
```

Figure 16-2 Menu 11.3 Remote Node Network Layer Options

Table 16-1 Menu 11.3 Remote Node Network Layer Options : Bridge Fields

FIELD	DESCRIPTION
Bridge (menu 11.1)	Make sure this field is set to **Yes**.
Edit IP/Bridge (menu 11.1)	Press [SPACE BAR] to select **Yes** and press [ENTER] to display menu 11.3.
Ethernet Addr Timeout (min.) (menu 11.3)	Type the time (in minutes) for the Prestige to retain the Ethernet Address information in its internal tables while the line is down. If this information is retained, your Prestige will not have to recompile the tables when the line comes back up.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

16.2.2 Bridge Static Route Setup

Similar to network layer static routes, a bridging static route tells the Prestige the route to a node before a connection is established. You configure bridge static routes in menu 12.3.1 (go to menu 12, choose option 3, then choose a static route to edit) as shown next.

```
                Menu 12.3.1 - Edit Bridge Static Route

                Route #: 1
                Route Name=
                Active= No
                Ether Address= ?
                IP Address=
                Gateway Node= 1



              Press ENTER to Confirm or ESC to Cancel:
```

Figure 16-3 Menu 12.3.1 Edit Bridge Static Route

The following table describes the **Edit Bridge Static Route** menu.

Table 16-2 Menu 12.3.1 Edit Bridge Static Route

FIELD	DESCRIPTION
Route #	This is the route index number you typed in **Menu 12.3 – Bridge Static Route Setup**.
Route Name	Type a name for the bridge static route for identification purposes.

Table 16-2 Menu 12.3.1 Edit Bridge Static Route

FIELD	DESCRIPTION
Active	Indicates whether the static route is active (**Yes**) or not (**No**).
Ether Address	Type the MAC address of the destination computer that you want to bridge the packets to.
IP Address	If available, type the IP address of the destination computer that you want to bridge the packets to.
Gateway Node	Press [SPACE BAR] and then [ENTER] to select the number of the remote node (one to eight) that is the gateway of this static route.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Chapter 17
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

17.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

17.2 Applying NAT

You apply NAT via menus 4 or 11.3 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. .

```
                Menu 4 - Internet Access Setup

        ISP's Name= MyISP
        Encapsulation= PPPoE
        Multiplexing= LLC-based
        VPI #= 1
        VCI #= 32
        ATM QoS Type= CBR
          Peak Cell Rate (PCR)= 0
          Sustain Cell Rate (SCR)= 0
          Maximum Burst Size (MBS)= 0
        My Login= 1234
        My Password= ********
        Idle Timeout (sec)= 0
        IP Address Assignment= Dynamic
          IP Address= N/A
        Network Address Translation= SUA Only
          Address Mapping Set= N/A
          Press ENTER to Confirm or ESC to Cancel: Press Space Bar to Toggle.
```

Figure 17-1 Menu 4 Applying NAT for Internet Access

Step 1. Enter 4 from the main menu..

Step 2. Move the cursor to the **Network Address Translation** field, press [SPACE BAR] to select **SUA Only.**

Step 3. Press [ENTER] to save your settings back to the Prestige.

The following figure shows how you apply NAT to the remote node in menu 11.1.

```
                Menu 11.3 - Remote Node Network Layer Options

IP Options:                              Bridge Options:
  IP Address Assignment = Dynamic          Ethernet Addr Timeout(min)= N/A
  Rem IP Addr = 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= N/A
  NAT= SUA Only
    Address Mapping Set= N/A
  Metric= 2
  Private= No
  RIP Direction= None
    Version= RIP-1
  Multicast= None
  IP Policies=


                  Enter here to CONFIRM or ESC to CANCEL:
```

Figure 17-2 Menu 11.3 Applying NAT to the Remote Node

Step 1. Enter 11 from the main menu.

Step 2. When menu 11 appears, as shown in the following figure, type the number of the remote node that you want to configure.

Step 3. Move the cursor to the Edit IP/Bridge field, press [SPACE BAR] to select Yes and then press [ENTER] to bring up Menu 11.3 - Remote Node Network Layer Options.

Select None to disable NAT **or** SUA Only **to enable the Address Mapping Set of menu 15.2.**

17.3 NAT Server Setup

A server set is a list of LAN servers mapped to external ports. To use this set, NAT must be enabled. Please see the section on port forwarding in the chapter on NAT web configurator screens for further information on these menus. To configure NAT Server Setup, enter 15 from the main menu to bring up the following screen.

```
                    Menu 15.2.1 - NAT Server Setup


 Rule   Start Port No.   End Port No.   IP Address
-------------------------------------------------
   1.    Default          Default        0.0.0.0
   2.      21               25           192.168.1.33
   3.      0                0            0.0.0.0
   4.      0                0            0.0.0.0
   5.      0                0            0.0.0.0
   6.      0                0            0.0.0.0
   7.      0                0            0.0.0.0
   8.      0                0            0.0.0.0
   9.      0                0            0.0.0.0
  10.      0                0            0.0.0.0
  11.      0                0            0.0.0.0
  12.      0                0            0.0.0.0

        Press ENTER to Confirm or ESC to Cancel:
```

Figure 17-3 Menu 15.2.1 NAT Server Setup

Step 1. Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.

Step 2. Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.

Step 3. Press [ENTER] at the "Press ENTER to confirm …" prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

17.4 General NAT Examples

The following are some examples of NAT configuration using the SMT.

17.4.1 Example 1: Internet Access

In the following Internet access example, one public IP address on the WAN is mapped to several private IP addresses on the LAN. Therefore these LAN computers are invisible to the outside world.

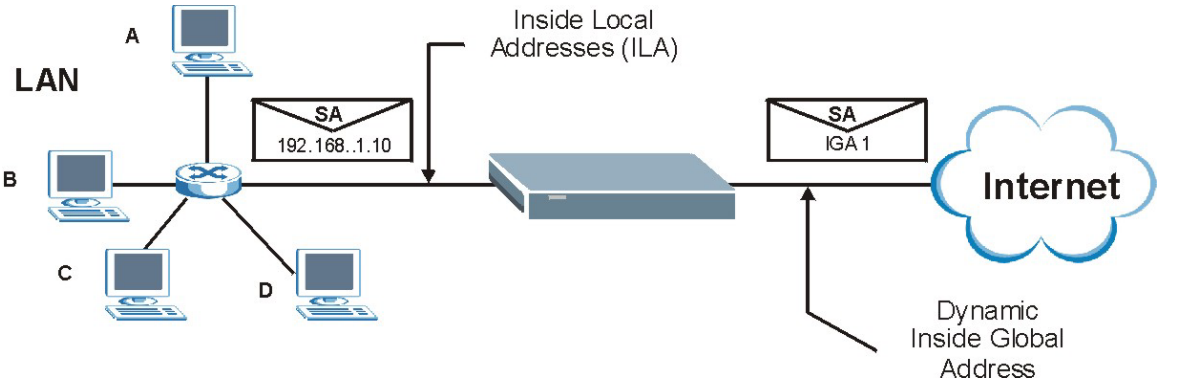


Figure 17-4 Configuring NAT

17.4.2 How to configure NAT

From menu 4, choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section 17.4.* The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

```
                Menu 4 - Internet Access Setup

        ISP's Name= MyISP
        Encapsulation= RFC 1483
        Multiplexing= LLC-based
        VPI #= 8
        VCI #= 35
        ATM QoS Type= UBR
          Peak Cell Rate (PCR)= 0
          Sustain Cell Rate (SCR)= 0
          Maximum Burst Size (MBS)= 0
        My Login= N/A
        My Password= N/A
        ENET ENCAP Gateway= N/A
        IP Address Assignment= Static
          IP Address= 0.0.0.0
        Network Address Translation= SUA Only
          Address Mapping Set= N/A

        Press ENTER to Confirm or ESC to Cancel:
```

Figure 17-5 Configuring NAT SMT Menus

17.4.3 Example 2: Configuring an Inside Server

In this case you want to make the LAN Server visible to the outside world.

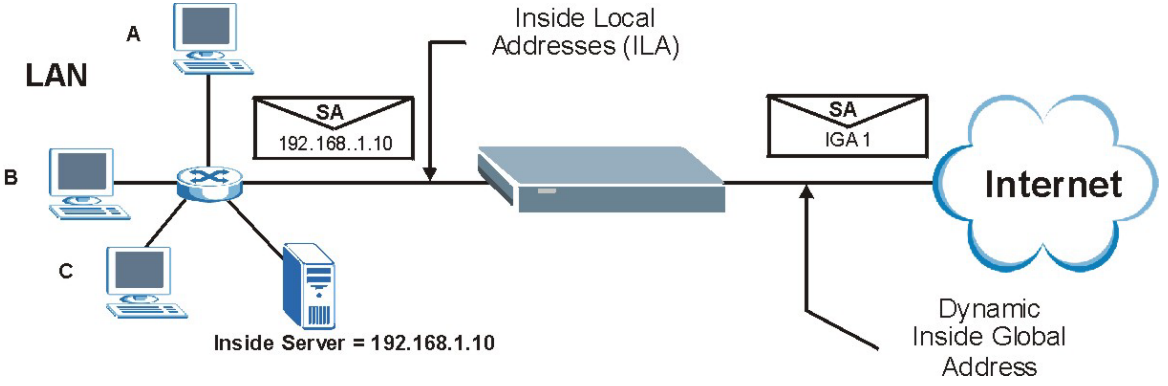


Figure 17-6 Configuring an Inside Server

17.4.4 How to configure an Inside Server

Go to menu 15.2 to specify the Inside Server behind the NAT as shown in the next figure.

```
Menu 15.2.1 - NAT Server Setup (Used for SUA Only)


 Rule    Start Port No.    End Port No.    IP Address
-------------------------------------------------------
   1.     Default           Default        192.168.1.10
   2.       0                 0            0.0.0.0
   3.       0                 0            0.0.0.0
   4.       0                 0            0.0.0.0
   5.       0                 0            0.0.0.0
   6.       0                 0            0.0.0.0
   7.       0                 0            0.0.0.0
   8.       0                 0            0.0.0.0
   9.       0                 0            0.0.0.0
  10.       0                 0            0.0.0.0
  11.       0                 0            0.0.0.0
  12.       0                 0            0.0.0.0

        Press ENTER to Confirm or ESC to Cancel:
```

Figure 17-7 Menu 15.2.1 Specifying an Inside Server

Part VII:

SMT Advanced Management

This part discusses filtering setup, SNMP, system information and diagnosis, firmware and configuration file maintenance, system maintenance, remote management, IP policy routing and call scheduling.

See the web configurator parts of this guide for background information on features configurable by web configurator and SMT.

Chapter 18
Filter Configuration

This chapter shows you how to create and apply filters.

18.1 About Filtering

Your Prestige uses filters to decide whether or not to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the Ethernet side. Call filtering is used to determine if a packet should be allowed to trigger a call.

Outgoing packets must undergo data filtering before they encounter call filtering. Call filters are divided into two groups, the built-in call filters and user-defined call filters. Your Prestige has built-in call filters that prevent administrative, for example, RIP packets from triggering calls. These filters are always enabled and not accessible to you. Your Prestige applies the built-in filters first and then the user-defined call filters, if applicable, as shown next.

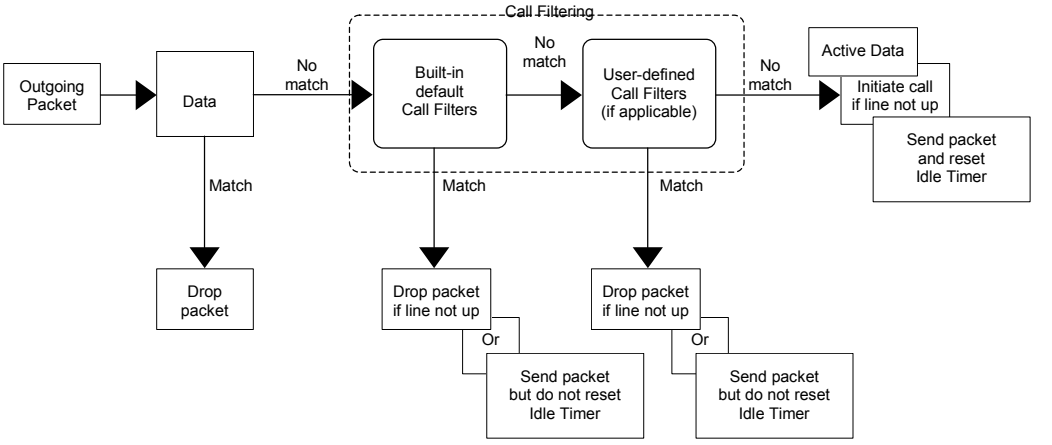


Figure 18-1 Outgoing Packet Filtering Process

Two sets of factory filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule.

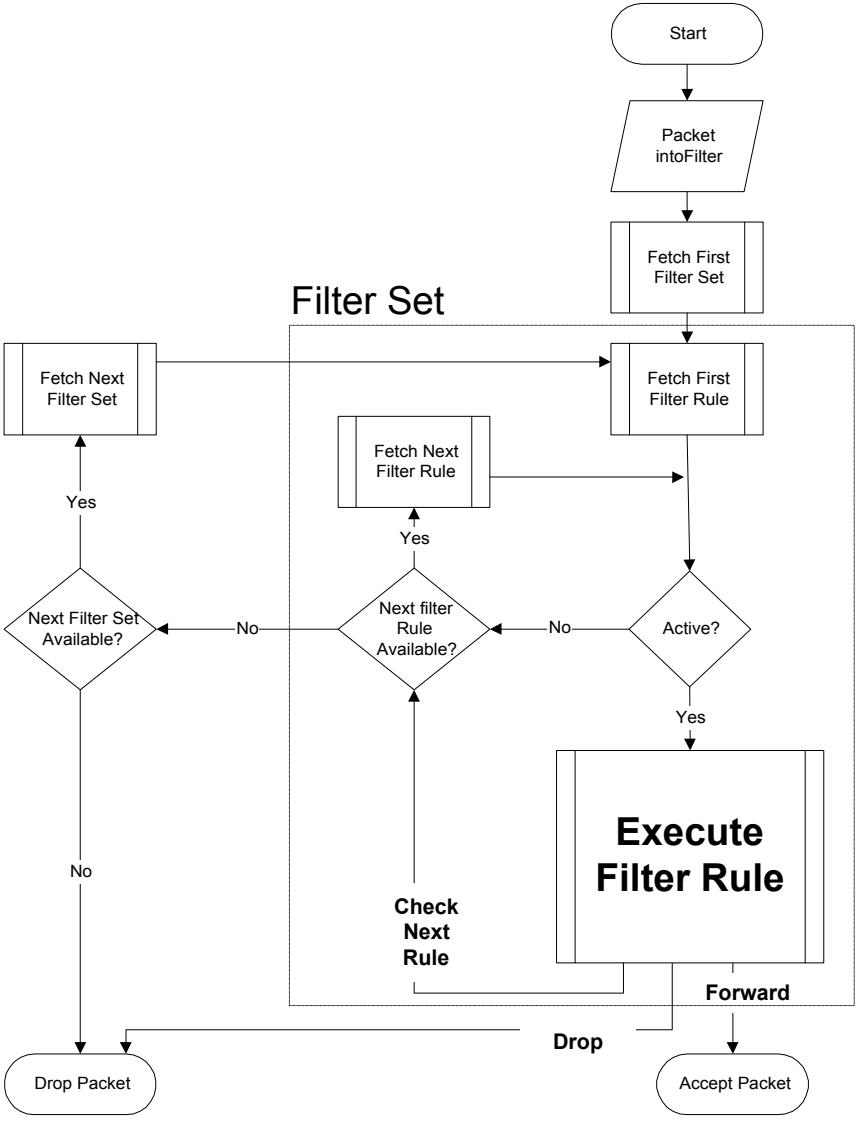


Figure 18-2 Filter Rule Process

You can apply up to four filter sets to a particular port to block various types of packets. Because each filter set can have up to six rules, you can have a maximum of 24 rules active for a single port.

For incoming packets, your Prestige applies data filters only. Packets are processed depending on whether a match is found. The following sections describe how to configure filter sets.

The Filter Structure of the Prestige

A filter set consists of one or more filter rules. Usually, you would group related rules, for example, all the rules for NetBIOS, into a single set and give it a descriptive name. You can configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.

18.2 Configuring a Filter Set

To configure a filter set, follow the steps shown next.

Step 1. Enter 21 in the main menu to display **Menu 21 – Filter Set Configuration**.

```
                Menu 21 - Filter Set Configuration

Filter                                Filter
Set #        Comments                 Set #        Comments
------  -----------------             ------  -----------------
  1      NetBIOS_WAN                     7      _________________
  2      NetBIOS_LAN                     8      _________________
  3      PPPoE                           9      _________________
  4                                     10      _________________
  5                                     11      _________________
  6      _________________              12      _________________

            Enter Filter Set Number to Configure= 0

            Edit Comments= N/A

            Press ENTER to Confirm or ESC to Cancel:
```

Figure 18-3 Menu 21 Filter Set Configuration

Step 2. Type the filter set to configure (no. 1 to 12) and press [ENTER].

Step 3. Type a descriptive name or comment in the **Edit Comments** field and press [ENTER].

Step 4. Press [ENTER] at the message "Press ENTER to confirm…" to display **Menu 21.1 – Filter Rules Summary** (that is, if you selected filter set 1 in menu 21).

```
                        Menu 21.1 - Filter Rules Summary

# A Type                          Filter Rules                              M m n
- - ---- ------------------------------------------------------------------ - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137                               N D N
2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138                               N D N
3 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139                               N D N
4 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137                              N D N
5 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138                              N D N
6 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139                              N D F


                  Enter Filter Rule Number (1-6) to Configure:
```

Figure 18-4 NetBIOS_WAN Filter Rules Summary

```
                        Menu 21.2 - Filter Rules Summary

# A Type                          Filter Rules                              M m n
- - ---- ------------------------------------------------------------------ - - -
1 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53                       N D F
2 N
3 N
4 N
5 N
6 N


                  Enter Filter Rule Number (1-6) to Configure:
```

Figure 18-5 NetBIOS_LAN Filter Rules Summary

```
                        Menu 21.4 - Filter Rules Summary

# A Type                          Filter Rules                              M m n
- - ---- ------------------------------------------------------------------ - - -
1 Y Gen  Off=12, Len=2, Mask=ffff, Value=8863                               N F N
2 Y Gen  Off=12, Len=2, Mask=ffff, Value=8864                               N F D
3 N
4 N
5 N
6 N


                  Enter Filter Rule Number (1-6) to Configure:
```

Figure 18-6 PPPoE Filter Rules Summary

18.2.1 Filter Rules Summary Menus

The following tables briefly describe the abbreviations used in menu 21.x.

Table 18-1 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
#	The filter rule number: 1 to 6.
A	Active: "Y" means the rule is active. "N" means the rule is inactive.
Type	The type of filter rule: "GEN" for Generic, "IP" for TCP/IP.
Filter Rules	These parameters are displayed here.
M	More. "Y" means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. "N" means there are no more rules to check. You can specify an action to be taken for instance, forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.
n	Action Not Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

Table 18-2 Rule Abbreviations Used

FILTER TYPE	DESCRIPTION
IP	
Pr	Protocol
SA	Source Address
SP	Source Port Number
DA	Destination Address
DP	Destination Port Number
GEN	

Table 18-2 Rule Abbreviations Used

FILTER TYPE	DESCRIPTION
Off	Offset
Len	Length

18.3 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.x – Filter Rules Summary** and press [ENTER] to open menu 21.x.1 for the rule.

There are two types of filter rules: **TCP/IP** and **Generic**. Depending on the type of rule, the parameters for each type will be different. Use [SPACE BAR] to select the type of rule that you want to create in the **Filter Type** field and press [ENTER] to open the respective menu.

To speed up filtering, all rules in a filter set must be of the same class, for instance, protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filters field or vice versa, the Prestige will warn you and will not allow you to save.

18.3.1 TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select TCP/IP Filter Rule from the **Filter Type** field and press [ENTER] to open **Menu 21.x.1 – TCP/IP Filter Rule**, as shown next.

```
                    Menu 21.6.1 - TCP/IP Filter Rule

                Filter #: 6,1
                Filter Type= TCP/IP Filter Rule
                Active= No
                IP Protocol= 0     IP Source Route= No
                Destination: IP Addr=
                             IP Mask=
                             Port #=
                             Port # Comp= None
                     Source: IP Addr=
                             IP Mask=
                             Port #=
                             Port # Comp= None
                TCP Estab= N/A
                More= No           Log= None
                Action Matched= Check Next Rule
                Action Not Matched= Check Next Rule

                Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Figure 18-7 Menu 21.x.1 TCP/IP Filter Rule

The following table describes how to configure your TCP/IP filter rule.

Table 18-3 Menu 21.x.1 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third filter rule of that set.	6,1
Filter Type	Use [SPACE BAR] and then [ENTER] to choose a rule. Parameters displayed for each type will be different. Choices are **TCP/IP Filter Rule** or **Generic Filter Rule**.	**TCP/IP Filter Rule**
Active	Select **Yes** to activate or **No** to deactivate the filter rule.	**No** (default)
IP Protocol	This is the upper layer protocol, for example, TCP is 6, UDP is 17 and ICMP is 1. The value must be between 0 and 255. A value of O matches ANY protocol.	0 to 255
IP Source Route	IP Source Route is an optional header that dictates the route an IP packet takes from its source to its destination. If **Yes**, the rule applies to any packet with an IP source route. The majority of IP packets do not have source route.	**No** (default)
Destination: IP Addr	Type the destination IP address of the packet you want to filter. This field is ignored if it is 0.0.0.0.	IP address

Table 18-3 Menu 21.x.1 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
IP Mask	Type the IP mask to apply to the Destination: IP Addr field.	IP mask
Port #	Type the destination port of the packets you want to filter. The field range is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in **Destination: Port #.** Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**.	**None**
Source: IP Addr	Type the source IP Address of the packet you want to filter. A 0.0.0.0 field is ignored.	IP address
IP Mask	Type the IP mask to apply to the **Source: IP Addr** field.	IP mask
Port #	Type the source port of the packets you want to filter. The range of this field is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the source port in the packet against the value given in **Source: Port #** field. Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**.	**None**
TCP Estab	This applies only when the IP Protocol field is 6, TCP. If **Yes**, the rule matches packets that want to establish TCP connection(s) (SYN=1 and ACK=0); else it is ignored.	**No** (default)
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be N/A.	**No** (default)
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** – Only packets that match the rule parameters will be logged. **Action Not Matched** – Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	**None**
Action Matched	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)

Table 18-3 Menu 21.x.1 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

The following figure illustrates the logic flow of an IP filter.

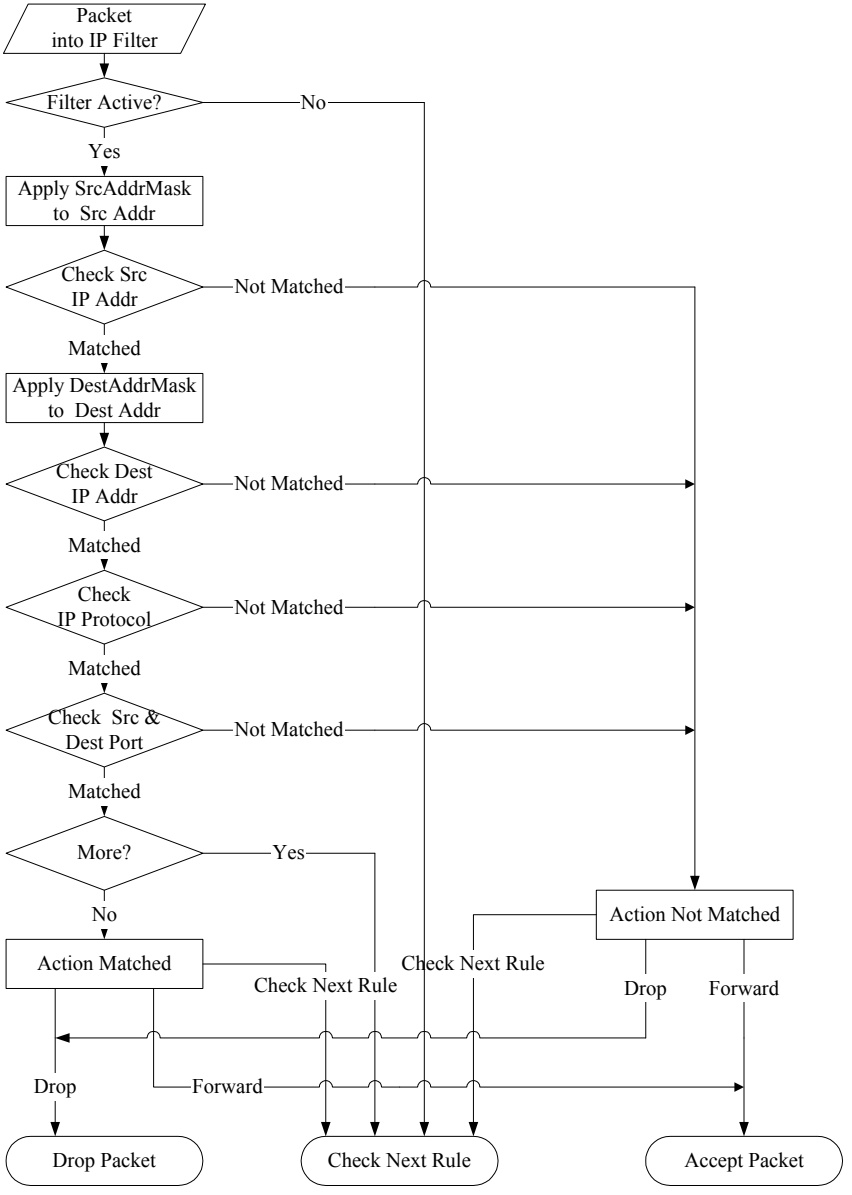


Figure 18-8 Executing an IP Filter

18.3.2 Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the Prestige treats a packet as a byte stream as opposed to an IP packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The Prestige applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** fields are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule select an empty filter set in menu 21, for example 6. Select **Generic Filter Rule** in the **Filter Type** field and press [ENTER] to open **Menu 21.6.1 – Generic Filter Rule**, as shown in the following figure.

```
                    Menu 21.6.1 - Generic Filter Rule

                Filter #: 6,1
                Filter Type= Generic Filter Rule
                Active= No
                Offset= 0
                Length= 0
                Mask= N/A
                Value= N/A
                More= No            Log= None
                Action Matched= Check Next Rule
                Action Not Matched= Check Next Rule

                Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 18-9 Menu 21.6.1 Generic Filter Rule

The next table describes the fields in the **Generic Filter Rule** menu.

Table 18-4 Menu 21.6.1 Generic Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third rule of that set.	6,1

Table 18-4 Menu 21.6.1 Generic Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Filter Type	Press [SPACE BAR] and then [ENTER] to select a type of rule. Parameters displayed below each type will be different. Choices are **Generic Filter Rule** or **TCP/IP Filter Rule**.	**Generic Filter Rule**
Active	Select **Yes** to turn on or **No** to turn off the filter rule.	**No** (default)
Offset	Type the starting byte of the data portion in the packet that you want to compare. The range for this field is from 0 to 255.	0 (default)
Length	Type the byte count of the data portion in the packet that you want to compare. The range for this field is 0 to 8.	0 (default)
Mask	Type the mask (in Hexadecimal) to apply to the data portion before comparison.	
Value	Type the value (in Hexadecimal) to compare with the data portion.	
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**.	**No** (default)
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** – Only matching packets and rules will be logged. **Action Not Matched** – Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	**None**
Action Matched	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

18.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** Device rules and Protocol Filter (**TCP/IP**) rules. Generic Filter rules act on the raw data from/to LAN and WAN. Protocol Filter rules act on IP packets.

When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the Prestige applies the protocol filters to the "native" IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic (or device) filters are applied to the raw packets that appear on the wire. They are applied at the point where the Prestige is receiving and sending the packets; for instance, the interface. The interface can be an Ethernet, or any other hardware port. The following figure illustrates this.

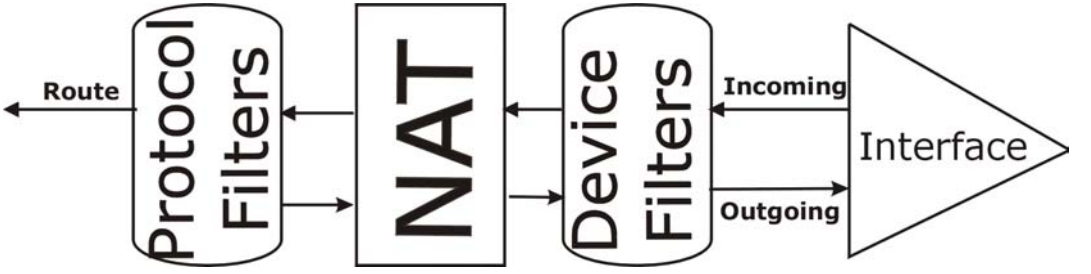


Figure 18-10 Protocol and Device Filter Sets

18.5 Example Filter

Let's look at an example to block outside telnet access to the Prestige.

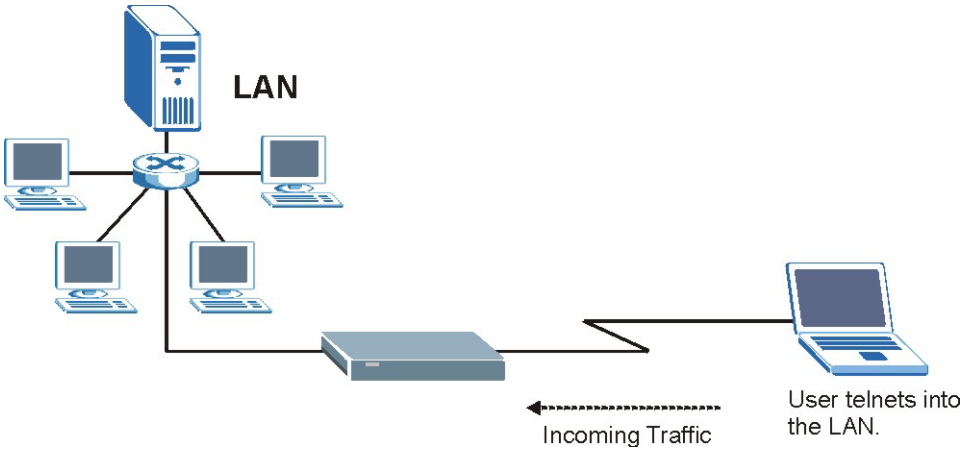


Figure 18-11 Sample Telnet Filter

Step 1. Enter 21 in the main menu to display **Menu 21 — Filter Set Configuration**.

Step 2. Enter the index number of the filter set you want to configure (in this case 3).

Step 3. Type a descriptive name or comment in the **Edit Comments** field (for example, TELNET_WAN) and press [ENTER].

Step 4. Press [ENTER] at the message "Press [ENTER] to confirm or [ESC] to cancel" to open **Menu 21.3 — Filter Rules Summary**.

Step 5. Type 1 to configure the first filter rule. Make the entries in this menu as shown next.

When you press [ENTER] to confirm, the following screen appears. Note that there is only one filter rule in this set.

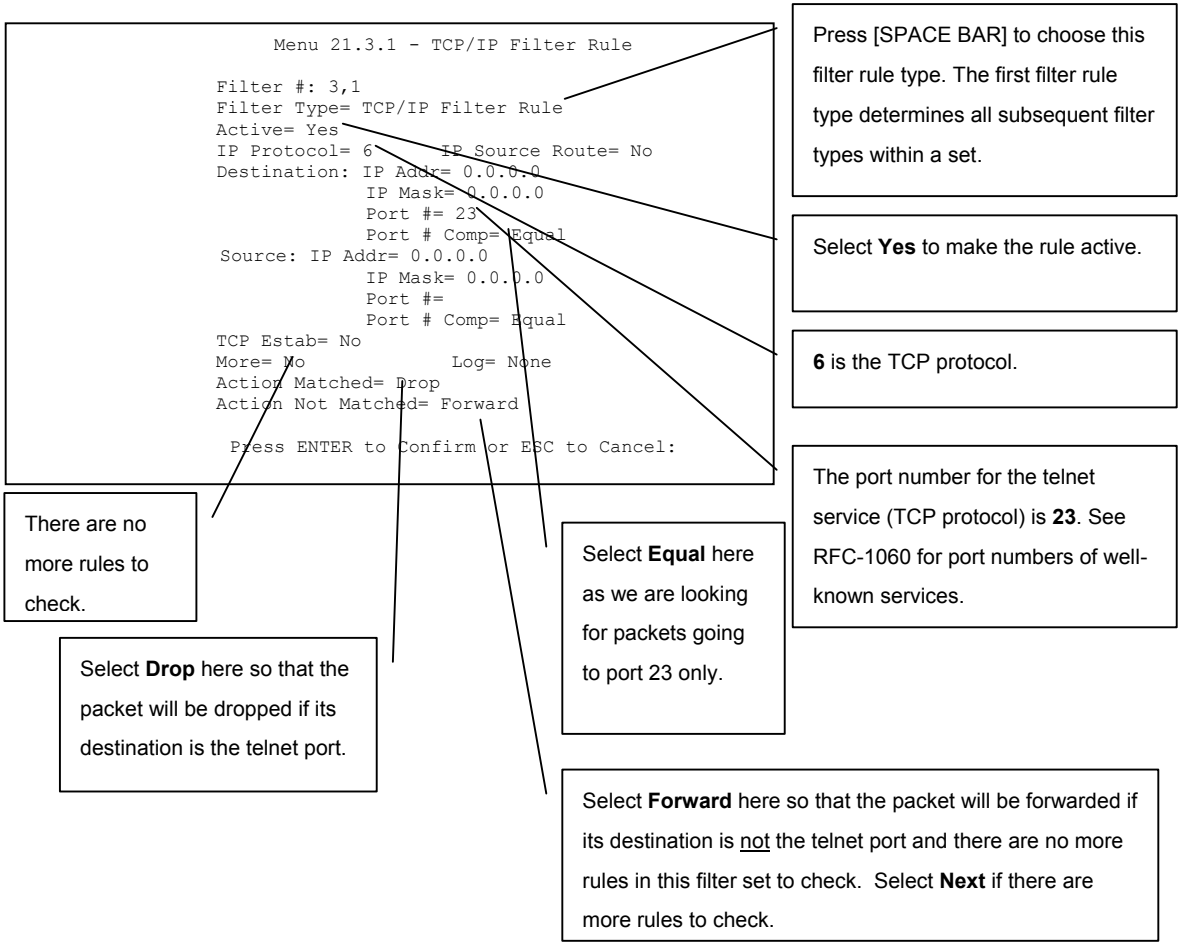

Menu 21.3.1 - TCP/IP Filter Rule
Filter #: 3,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6 IP Source Route= No
Destination: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #= 23
Port # Comp= Equal
Source: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #=
Port # Comp= Equal
TCP Estab= No
More= No Log= None
Action Matched= Drop
Action Not Matched= Forward
Press ENTER to Confirm or ESC to Cancel:
Press [SPACE BAR] to choose this filter rule type. The first filter rule type determines all subsequent filter types within a set.
Select Yes to make the rule active.
6 is the TCP protocol.
The port number for the telnet service (TCP protocol) is 23. See RFC-1060 for port numbers of well-known services.
There are no more rules to check.
Select Drop here so that the packet will be dropped if its destination is the telnet port.
Select Equal here as we are looking for packets going to port 23 only.
Select Forward here so that the packet will be forwarded if its destination is not the telnet port and there are no more rules in this filter set to check. Select Next if there are more rules to check.

Figure 18-12 Menu 21.3.1 Sample Filter

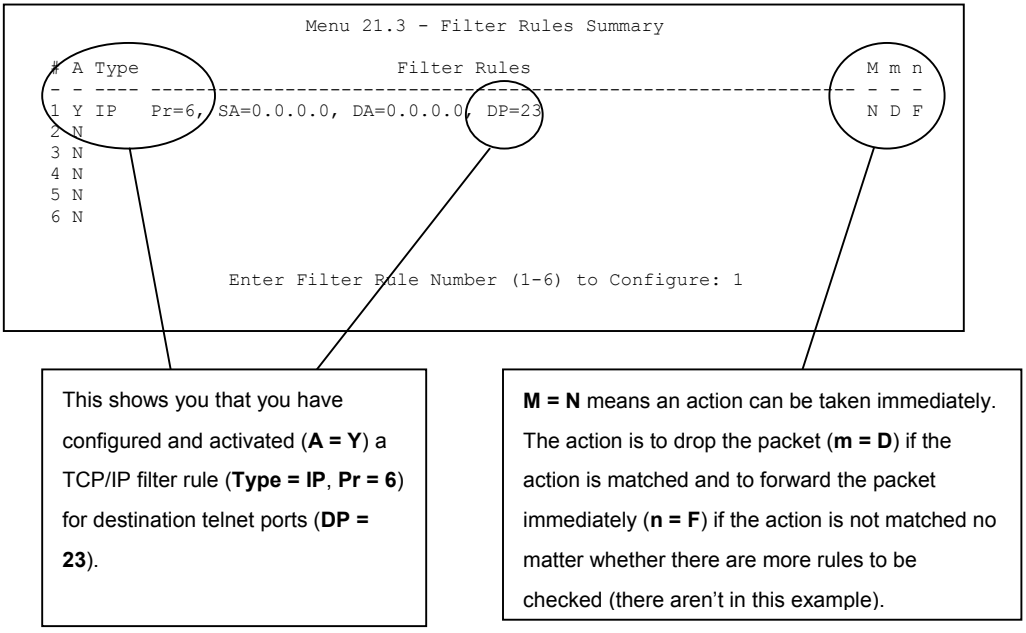

Menu 21.3 - Filter Rules Summary
A Type Filter Rules M m n
1 Y IP Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23 N D F
2 N
3 N
4 N
5 N
6 N
Enter Filter Rule Number (1-6) to Configure: 1
This shows you that you have configured and activated (A = Y) a TCP/IP filter rule (Type = IP, Pr = 6) for destination telnet ports (DP = 23).
M = N means an action can be taken immediately. The action is to drop the packet (m = D) if the action is matched and to forward the packet immediately (n = F) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

Figure 18-13 Menu 21.3 Sample Filter Rules Summary

After you have created the filter set, you must apply it.

Step 1. Enter 11 in the main menu to display menu 11 and type the remote node number to edit.

Step 2. Go to the **Edit Filter Sets** field, press [SPACE BAR] to choose **Yes** and press [ENTER].

Step 3. This brings you to menu 11.5. Apply the example filter set (for example, filter set 3) in this menu as shown in the next section.

18.6 Applying Filters and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them). Sets of factory default filter rules have been configured in menu 21 (but have not been applied) to filter traffic.

Table 18-5 Filter Sets Table

FILTER SETS	DESCRIPTION
Input Filter Sets:	Apply filters for incoming traffic. You may apply protocol or device filter rules. See earlier in this chapter for information on filters.
Output Filter Sets:	Apply filters for traffic leaving the Prestige. You may apply filter rules for protocol or device filters. See earlier in this section for information on types of filters.
Call Filter Sets:	Apply filters to decide if a packet should be allowed to trigger a call.

18.6.1 Ethernet Traffic

You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and type the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by typing their numbers separated by commas, for example, 2, 4, 6, 11. The factory default filter set, NetBIOS_LAN, is inserted in the **protocol filters** field under **Input Filter Sets** in menu 3.1 in order to prevent local NetBIOS messages from triggering calls to the DNS server.

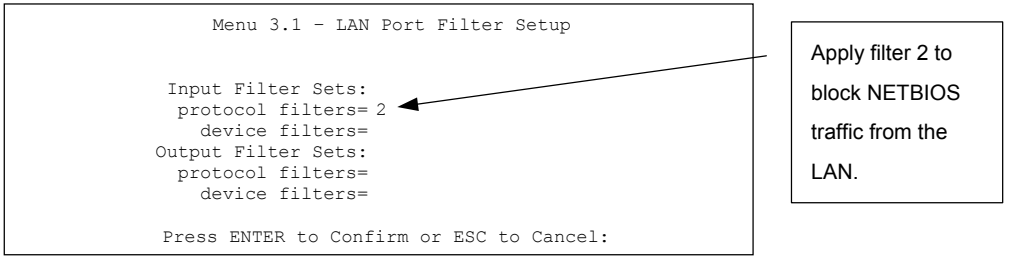

Menu 3.1 - LAN Port Filter Setup
Input Filter Sets:
protocol filters= 2
device filters=
Output Filter Sets:
protocol filters=
device filters=
Press ENTER to Confirm or ESC to Cancel:
Apply filter 2 to block NETBIOS traffic from the LAN.

Figure 18-14 Filtering Ethernet Traffic

18.6.2 Remote Node Filters

Go to menu 11.5 (shown next) and type the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by typing their numbers separated by commas. The factory default filter set, NetBIOS_WAN, is inserted in the **protocol filters** field under **Call Filter Sets** in menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP.

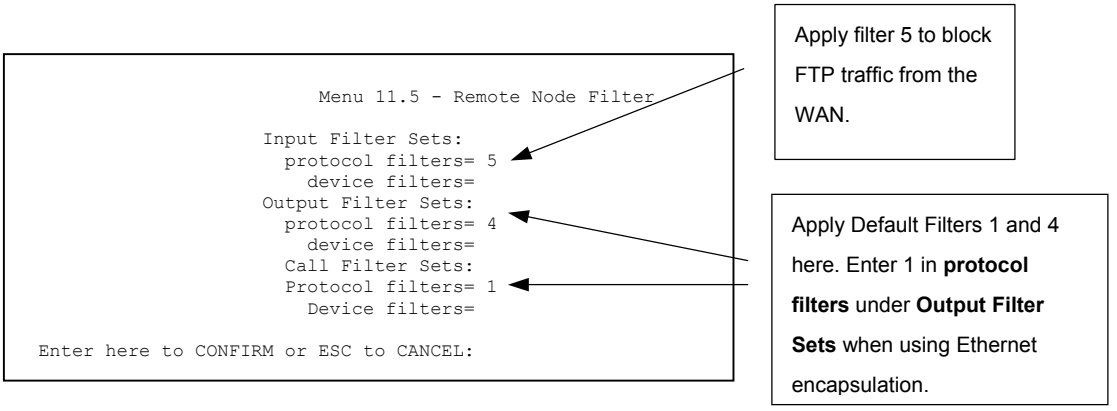

Menu 11.5 - Remote Node Filter
Input Filter Sets:
protocol filters= 5
device filters=
Output Filter Sets:
protocol filters= 4
device filters=
Call Filter Sets:
Protocol filters= 1
Device filters=
Enter here to CONFIRM or ESC to CANCEL:
Apply filter 5 to block FTP traffic from the WAN.
Apply Default Filters 1 and 4 here. Enter 1 in **protocol filters** under **Output Filter Sets** when using Ethernet encapsulation.

Figure 18-15 Filtering Remote Node Traffic

Note that call filter sets are visible when you select PPPoA or PPPoE encapsulation.

Chapter 19
SNMP Configuration

This chapter explains SNMP Configuration menu 22.

19.1 SNMP Overview

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. The Prestige supports SNMP version one (SNMPv1) and version two c (SNMPv2c). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

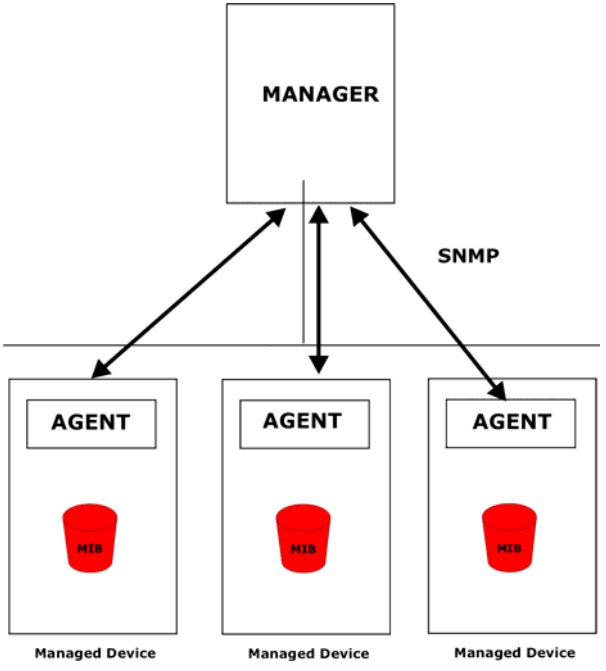


Figure 19-1 SNMP Management Model

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed device (the Prestige). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include the number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

19.2 Supported MIBs

The Prestige supports RFC-1215 and MIB II as defined in RFC-1213 as well as ZyXEL private MIBs. The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

19.3 SNMP Configuration

To configure SNMP, select option 22 from the main menu to open **Menu 22 — SNMP Configuration** as shown next. The "community" for Get, Set and Trap fields is SNMP terminology for password.

```
                    Menu 22 - SNMP Configuration

                SNMP:
                  Get Community= public
                  Set Community= public
                  Trusted Host= 0.0.0.0
                  Trap:
                    Community= public
                    Destination= 0.0.0.0


                  Press ENTER to Confirm or ESC to Cancel:
```

Figure 19-2 Menu 22 SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 19-1 Menu 22 SNMP Configuration

FIELD	DESCRIPTION	EXAMPLE
SNMP:		
Get Community	Type the **Get Community**, which is the password for the incoming Get- and GetNext requests from the management station.	public
Set Community	Type the **Set** community, which is the password for incoming Set requests from the management station.	public
Trusted Host	If you enter a trusted host, your Prestige will only respond to SNMP messages from this address. A blank (default) field means your Prestige will respond to all SNMP messages it receives, regardless of source.	0.0.0.0
Trap:		
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.	public
Destination	Type the IP address of the station to send your SNMP traps to.	0.0.0.0
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

19.4 SNMP Traps

The Prestige will send traps to the SNMP manager when any one of the following events occurs:

Table 19-2 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (*defined in RFC-1215*)	A trap is sent after booting (power on).
2	warmStart (*defined in RFC-1215*)	A trap is sent after booting (software reboot).
3	linkDown (*defined in RFC-1215*)	A trap is sent when the port is down.
4	linkUp (*defined in RFC-1215*)	A trap is sent when the port is up.
5	authenticationFailure (*defined in RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot :	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).

The following table maps the physical port and encapsulation to the interface type.

Table 19-3 Ports and Interface Types

PHYSICAL PORT/ENCAP	INTERFACE TYPE
LAN port(s)	enet0
Wireless port	enet1
PPPoE encap	pppoe
1483 encap	mpoa
Ethernet encap	enet-encap
PPPoA	ppp

Chapter 20
System Information and Diagnosis

This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.4 and menu 24.8.

20.1 System Maintenance Overview

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type 24 in the main menu to open **Menu 24 – System Maintenance**, as shown in the following figure.

```
Menu 24 - System Maintenance

1.  System Status
2.  System Information and Console Port Speed
3.  Log and Trace
4.  Diagnostic
5.  Backup Configuration
6.  Restore Configuration
7.  Upload Firmware
8.  Command Interpreter Mode
9.  Call Control
10. Time and Date Setting
11. Remote Management

Enter Menu Selection Number:
```

Figure 20-1 Menu 24 System Maintenance

20.2 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next. System Status is a tool that can be used to monitor your Prestige. Specifically, it gives you information on your ADSL telephone line status, number of packets sent and received.

To get to System Status, type 24 to go to **Menu 24 — System Maintenance.** From this menu, type 1**. System Status**. There are two commands in **Menu 24.1 — System Maintenance — Status**. Entering 1 resets the counters; pressing [TAB] toggles between Ethernet and USB port status display and [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status** which are read-only and meant for diagnostic purposes.

```
                    Menu 24.1 - System Maintenance - Status          07:05:39
                                                                Sat. Jan. 01, 2000

Node-Lnk Status      TxPkts      RxPkts      Errors  Tx B/s  Rx B/s     Up Time
 1-PPPoE Idle             0           0           0       0       0     0:00:00
 2       N/A              0           0           0       0       0     0:00:00
 3       N/A              0           0           0       0       0     0:00:00
 4       N/A              0           0           0       0       0     0:00:00
 5       N/A              0           0           0       0       0     0:00:00
 6       N/A              0           0           0       0       0     0:00:00
 7       N/A              0           0           0       0       0     0:00:00
 8       N/A              0           0           0       0       0     0:00:00

My WAN IP (from ISP): 0.0.0.0

    Ethernet:                                   WAN:
      Status: 100M/Full Duplex Tx Pkts: 2074      Line Status: Down
      Collisions: 0            Rx Pkts: 2665      Upstream Speed:     0 kbps
    CPU Load =   16.44%                           Downstream Speed:   0 kbps
                                  Press Command:
                COMMANDS: 1-Reset Counters  TAB-Next Page  ESC-Exit
```

Figure 20-2 Menu 24.1 System Maintenance : Status

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status**.

Table 20-1 Menu 24.1 System Maintenance : Status

FIELD	DESCRIPTION
Node-Lnk	This is the node index number and link type.
Status	This shows the status of the remote node.
TxPkts	The number of transmitted packets to this remote node.
RxPkts	The number of received packets from this remote node.
Errors	The number of error packets on this connection.
Tx B/s	This shows the transmission rate in bytes per second.
Rx B/s	This shows the receiving rate in bytes per second.
Up Time	This is the time this channel has been connected to the current remote node.
My WAN IP (from ISP)	This is the IP address of the ISP remote node.
Ethernet	This is the Ethernet or USB port. Press [TAB] to toggle between Ethernet and USB port status display.

Table 20-1 Menu 24.1 System Maintenance : Status

FIELD	DESCRIPTION
Status	This shows the current status of the LAN.
Tx Pkts	This is the number of transmitted packets to the LAN.
Rx Pkts	This is the number of received packets from the LAN.
Collision	This is the number of collisions.
WAN	This shows statistics for the WAN.
Line Status	This shows the current status of the xDSL line which can be **Up** or **Down**.
Upstream Speed	This shows the upstream transfer rate in kbps.
Downstream Speed	This shows the downstream transfer rate in kbps.
CPU Load	This specifies the percentage of CPU utilization.

20.3 System Information

To get to the System Information :

Step 1. Enter 24 in the main menu to display **Menu 24 — System Maintenance**.

Step 2. Enter 2 to display **Menu 24.2 — System Information**.

Step 3. From this menu you have two choices as shown in the next figure:

```
Menu 24.2 - System Information and Console Port Speed
      1. System Information
      2. Console Port Speed



            Please enter selection:
```

Figure 20-3 Menu 24.2 System Information and Console Port Speed

20.3.1 System Information

Enter 1 in menu 24.2 to display the screen shown next.

```
Menu 24.2.1 - System Maintenance - Information

     Name: p623me-t1
     Routing: IP/BRIDGE
     ZyNOS F/W Version: V3.40(QB.0)b1 | 12/18/2003
     ADSL Chipset Vendor:  TrendChip, Version  0.2.15. ASIC 1.1 +
     Standard: Multi-Mode

     LAN
       Ethernet Address: 00:a0:c5:01:23:45
       IP Address: 192.168.1.1
       IP Mask: 255.255.255.248
       DHCP: Server


         Press ESC or RETURN to Exit:
```

Figure 20-4 Menu 24.2.1 System Maintenance : Information

The following table describes the fields in this menu.

Table 20-2 Menu 24.2.1 System Maintenance : Information

FIELD	DESCRIPTION
Name	This displays the system name of your Prestige. This information can be changed in **Menu 1 – General Setup**.
Routing	This refers to the routing protocol used.
ZyNOS F/W Version	This refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
ADSL Chipset Vendor	This displays the vendor of the ADSL chipset and DSL version.
Standard	This refers to the operational protocol the Prestige and the DSLAM (Digital Subscriber Line Access Multiplexer) are using.
LAN	
Ethernet Address	This refers to the Ethernet MAC (Media Access Control) of your Prestige.
IP Address	This is the IP address of the Prestige in dotted decimal notation.
IP Mask	This shows the subnet mask of the Prestige.
DHCP	This field shows the DHCP setting (None, Relay or Server) of the Prestige.

20.3.2 Console Port Speed

The Prestige has an internal console port for support personnel only. Do not open the Prestige as it will void your warranty.

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your Prestige supports 9600 (default), 19200, 38400, 57600 and 115200 bps. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

```
Menu 24.2.2 – System Maintenance – Change Console Port Speed

                Console Port Speed: 9600

            Press ENTER to Confirm or ESC to Cancel:
```

Figure 20-5 Menu 24.2.2 System Maintenance : Change Console Port Speed

Once you change the Prestige consol port speed, you must also set the speed parameter for the communication software you are using to connect to the Prestige.

20.4 Log and Trace

There are two logging facilities in the Prestige. The first is the error logs and trace records that are stored locally. The second is the UNIX syslog facility for message logging.

20.4.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error log. Follow the procedures to view the local error/trace log:

Step 1. Type 24 in the main menu to display **Menu 24 – System Maintenance**.

Step 2. From menu 24, type 3 to display **Menu 24.3 – System Maintenance – Log and Trace**.

```
Menu 24.3 - System Maintenance - Log and Trace

   1. View Error Log
   2. UNIX Syslog


            Please enter selection:
```

Figure 20-6 Menu 24.3 System Maintenance : Log and Trace

Step 3. Enter 1 from **Menu 24.3 — System Maintenance — Log and Trace** to display the error log in the system.

After the Prestige finishes displaying the error log, you will have the option to clear it. Samples of typical error and information messages are presented in the next figure.

```
  59 Thu Jan 01 00:00:03 1970 PP0f  INFO  LAN promiscuous mode <0>
  60 Thu Jan 01 00:00:03 1970 PP00 -WARN  SNMP TRAP 0: cold start
  61 Thu Jan 01 00:00:03 1970 PP00  INFO  main: init completed
  62 Thu Jan 01 00:00:19 1970 PP00  INFO  SMT Session Begin
  63 Thu Jan 01 00:00:24 1970 PP0a  WARN  MPOA Link Down
Clear Error Log (y/n):
```

Figure 20-7 Sample Error and Information Messages

20.4.2 Syslog and Accounting

The Prestige uses the UNIX syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 — System Maintenance — UNIX Syslog**, as shown next.

```
            Menu 24.3.2 - System Maintenance - UNIX Syslog

                  UNIX Syslog:
                    Active= No
                    Syslog IP Address= 0.0.0.0
                    Log Facility= Local 1

                  Types:
                    CDR= No
                    Packet Triggered= No
                    Filter Log= No
                    PPP Log= No

               Press ENTER to Confirm or ESC to Cancel:
```

Figure 20-8 Menu 24.3.2 System Maintenance : UNIX Syslog

You need to configure the UNIX syslog parameters described in the following table to activate syslog then choose what you want to log.

Table 20-3 Menu 24.3.2 System Maintenance : UNIX Syslog

PARAMETER	DESCRIPTION
UNIX Syslog:	
Active	Use [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog IP Address	Type the IP address of your syslog server.

Table 20-3 Menu 24.3.2 System Maintenance : UNIX Syslog

PARAMETER	DESCRIPTION
Log Facility	Use [SPACE BAR] and then [ENTER] to select one of seven different local options. The log facility lets you log the message in different server files. Refer to your UNIX manual.
Types:	
CDR	Call Detail Record (CDR) logs all data phone line activity if set to **Yes.**
Packet triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to **Yes.**
Filter log	No filters are logged when this field is set to **No.** Filters with the individual filter **Log Filter** field set to **Yes** are logged when this field is set to **Yes.**
PPP log	PPP events are logged when this field is set to **Yes.**

Your Prestige sends four types of syslog messages. Some examples of these syslog messages with their message formats are shown next:

1. CDR

CDR Message Format

```
        SdcmdSyslogSend( SYSLOG_CDR, SYSLOG_INFO, String );
        String = board xx line xx channel xx, call xx, str
        board = the hardware board ID
        line = the WAN ID in a board
        Channel = channel ID within the WAN
        call = the call reference number which starts from 1 and increments by 1 for each new call
        str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)
                  L02     Tunnel Connected(L2TP)
                  C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call
Number)
                  L02 Call Terminated
                  C02 Call Terminated
```

```
Jul 19 11:19:27 192.168.102.2 ZyXEL Communications Corp.: board 0 line 0 channel 0, call
1, C01 Outgoing Call dev=2 ch=0 40002

Jul 19 11:19:32 192.168.102.2 ZyXEL Communications Corp.: board 0 line 0 channel 0, call
1, C02 OutCall Connected 64000 40002

Jul 19 11:20:06 192.168.102.2 ZyXEL Communications Corp.: board 0 line 0 channel 0, call
1, C02 Call Terminated
```

2. Packet triggered

Packet triggered Message Format

```
sdcmdSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String );
        String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x
        Protocol: (1:IP 2:BPDU 3:ATALK 4:IPNG)
        Data: We will send forty-eight Hex characters to the server
```

```
Jul 19 11:28:39 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c0200010061626364656667686 96a6b6c6d6e6
f7071727374

Jul 19 11:28:56 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd4000002040
5b4

Jul 19 11:29:06 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
```

3. Filter log

Filter log Message Format
SdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String); String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD IP[…] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m) drop (D). Src: Source Address Dst: Destination Address prot: Protocol ("TCP","UDP","ICMP") spo: Source port dpo: Destination port

```
Jul 19 14:43:55 192.168.102.2 ZyXEL Communications Corp.: IP[Src=202.132.154.123
Dst=255.255.255.255 UDP spo=0208  dpo=0208]}S03>R01mF

Jul 19 14:44:00 192.168.102.2 ZyXEL Communications Corp.: IP[Src=192.168.102.20
Dst=202.132.154.1 UDP spo=05d4  dpo=0035]}S03>R01mF

Jul 19 14:44:04 192.168.102.2 ZyXEL Communications Corp.: IP[Src=192.168.102.20

Dst=202.132.154.1 UDP spo=05d4  dpo=0035]}S03>R01mF
```

4. PPP log

PPP Log Message Format
sdcmdSyslogSend(SYSLOG_PPPLOG, SYSLOG_NOTICE, String); String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP /

```
Jul 19 11:42:44 192.168.102.2 ZyXEL Communications Corp.: ppp:LCP Closing

Jul 19 11:42:49 192.168.102.2 ZyXEL Communications Corp.: ppp:IPCP Closing

Jul 19 11:42:54 192.168.102.2 ZyXEL Communications Corp.: ppp:CCP Closing
```

20.5 Diagnostic

The diagnostic facility allows you to test the different aspects of your Prestige to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in the following figure.

Follow the procedure next to get to Diagnostic:

Step 1. From the main menu, type 24 to open **Menu 24 – System Maintenance**.

Step 2. From this menu, type 4. Diagnostic to open **Menu 24.4 – System Maintenance – Diagnostic**.

```
                Menu 24.4 - System Maintenance - Diagnostic

xDSL                                System
1.  Reset xDSL                      21. Reboot System
                                    22. Command Mode

TCP/IP
12. Ping Host


                        Enter Menu Selection Number:
                    Host IP Address= N/A
```

Figure 20-9 Menu 24.4 System Maintenance : Diagnostic

The following table describes the diagnostic tests available in menu 24.4 for and the connections.

Table 20-4 Menu 24.4 System Maintenance Menu : Diagnostic

FIELD	DESCRIPTION
Reset xDSL	Re-initialize the xDSL link to the telephone company.
Ping Host	Ping the host to see if the links and TCP/IP protocol on both systems are working.
Reboot System	Reboot the Prestige.
Command Mode	Type the mode to test and diagnose your Prestige using specified commands.
Host IP Address	If you typed 12 to Ping Host, now type the address of the computer you want to ping.

Chapter 21
Firmware and Configuration File Maintenance

This chapter tells you how to backup and restore your configuration file as well as upload new firmware and configuration files.

21.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the Prestige's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

Only use firmware for your Prestige's specific model. Refer to the label on the bottom of your Prestige.

```
ftp> put firmware.bin ras
```
This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the Prestige.

```
ftp> get rom-0 config.cfg
```
This is a sample FTP session saving the current configuration to the computer file "config.cfg".

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the Prestige only recognizes "rom-0" and "ras". Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the Prestige and the external filename refers to the filename not on the Prestige, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **ZyNOS F/W Version** field in **Menu 24.2.1 – System Maintenance – Information** to confirm that you have uploaded the correct firmware version. The AT command is the command you enter after you press "y" when prompted in the SMT menu to go into debug mode.

Table 21-1 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the Prestige. Uploading the rom-0 file replaces the entire ROM file system, including your Prestige configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the Prestige.	*.bin

21.2 Backup Configuration

The Prestige displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2; depending on whether you use the console port or Telnet.

Option 5 from **Menu 24 – System Maintenance** allows you to backup the current Prestige configuration to your computer. Backup is highly recommended once your Prestige is functioning properly. FTP is the preferred methods for backing up your current configuration to your computer since they are faster.

Please note that terms "download" and "upload" are relative to the computer. Download means to transfer from the Prestige to the computer, while upload means from your computer to the Prestige.

21.2.1 Backup Configuration

Follow the instructions as shown in the next screen.

```
                    Menu 24.5 - Backup Configuration

To transfer the configuration file to your computer, follow the procedure
below:

  1. Launch the FTP client on your computer.
  2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
  3. Locate the 'rom-0' file.
  4. Type 'get rom-0' to back up the current system configuration to your
     computer.

For details on FTP commands, please consult the documentation of your FTP
client program.  For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your user manual.

                            Press ENTER to Exit:
```

Figure 21-1 Telnet in Menu 24.5

21.2.2 Using the FTP Command from the Command Line

Step 1. Launch the FTP client on your computer.

Step 2. Enter "open", followed by a space and the IP address of your Prestige.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is "1234").

Step 5. Enter "bin" to set transfer mode to binary.

Step 6. Use "get" to transfer files from the Prestige to the computer, for example, "get rom-0 config.rom" transfers the configuration file on the Prestige to your computer and renames it "config.rom". See earlier in this chapter for more information on filename conventions.

Step 7. Enter "quit" to exit the ftp prompt.

21.2.3 Example of FTP Commands from the Command Line

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 21-2 FTP Session Example

21.2.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 21-2 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	You must use binary mode when uploading the configuration or firmware file. Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

21.2.5 TFTP and FTP over WAN Will Not Work When

TFTP, FTP and Telnet over WAN will not work when:

1. You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
2. You have an SMT console session running.

21.2.6 Backup Configuration Using TFTP

The Prestige supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

Step 1. Use telnet from your computer to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.

Step 2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

Step 3. Enter command "sys stdio 0" to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command "sys stdio 5" to restore the five-minute SMT timeout (default) when the file transfer is complete.

Step 4. Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.

Step 5. Use the TFTP client (see the example below) to transfer files between the Prestige and the computer. The file name for the configuration file is "rom-0" (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "get" to transfer from the Prestige to the computer and "binary" to set binary transfer mode.

21.2.7 TFTP Command Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the Prestige IP address, "get" transfers the file source on the Prestige (rom-0, name of the configuration file on the Prestige) to the file destination on the computer and renames it config.rom.

21.2.8 GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 21-3 General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the Prestige. 192.168.1.1 is the Prestige's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the Prestige and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the Prestige. The filename for the firmware is "ras" and for the configuration file, is "rom-0".
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

Refer to *section 21.2.5* to read about configurations that disallow TFTP and FTP over WAN.

21.3 Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your Prestige since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

WARNING!
DO NOT INTERRUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR PRESTIGE.

21.3.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

```
                    Menu 24.6 - Restore Configuration

To transfer the firmware and the configuration file, follow the procedure
below:

  1. Launch the FTP client on your computer.
  2. Type "open" and the IP address of your system.  Then type "root" and
     SMT password as requested.
  3. Type "put backupfilename rom-0" where backupfilename is the name of
     your backup configuration file on your computer and rom-0 is the
     remote file name on the system. This restores the configuration to
     your system.
  4. The system reboots automatically after a successful file transfer.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on restoring using TFTP (note that you must
remain on this menu to restore using TFTP), please see your user manual.

                            Press ENTER to Exit:
```

Figure 21-3 Telnet into Menu 24.6

Step 1. Launch the FTP client on your computer.

Step 2. Enter "open", followed by a space and the IP address of your Prestige.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is "1234").

Step 5. Enter "bin" to set transfer mode to binary.

Step 6. Find the "rom" file (on your computer) that you want to restore to your Prestige.

Step 7. Use "put" to transfer files from the Prestige to the computer, for example, "put config.rom rom-0" transfers the configuration file "config.rom" on your computer to the Prestige. See earlier in this chapter for more information on filename conventions.

Step 8. Enter "quit" to exit the ftp prompt. The Prestige will automatically restart after a successful restore process.

21.3.2 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Figure 21-4 Restore Using FTP Session Example

Refer to *section 21.2.5* to read about configurations that disallow TFTP and FTP over WAN.

21.4 Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the previous *Restore Configuration* section or by following the instructions in **Menu 24.7.2 – System Maintenance – Upload System Configuration File** (for console port).

WARNING!
DO NOT INTERRUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR PRESTIGE.

21.4.1 Firmware File Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the Prestige, you will see the following screens for uploading firmware and the configuration file using FTP.

```
          Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system.  Then type "root" and
     SMT password as requested.
  3. Type "put firmwarefilename ras" where "firmwarefilename" is the name
     of your firmware upgrade file on your workstation and "ras" is the
     remote file name on the system.
  4. The system reboots automatically after a successful firmware upload.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.
                            Press ENTER to Exit:
```

Figure 21-5 Telnet Into Menu 24.7.1 Upload System Firmware

21.4.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

```
     Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
  3. Type "put configurationfilename rom-0" where "configurationfilename"
     is the name of your system configuration file on your workstation, which
     will be transferred to the "rom-0" file on the system.
  4. The system reboots automatically after the upload system configuration
     file process is complete.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.

                           Press ENTER to Exit:
```

Figure 21-6 Telnet Into Menu 24.7.2 System Maintenance

To upload the firmware and the configuration file, follow these examples

21.4.3 FTP File Upload Command from the DOS Prompt Example

Step 1. Launch the FTP client on your computer.

Step 2. Enter "open", followed by a space and the IP address of your Prestige.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is "1234").

Step 5. Enter "bin" to set transfer mode to binary.

Step 6. Use "put" to transfer files from the computer to the Prestige, for example, "put firmware.bin ras" transfers the firmware on your computer (firmware.bin) to the Prestige and renames it "ras". Similarly, "put config.rom rom-0" transfers the configuration file on your computer (config.rom) to the Prestige and renames it "rom-0". Likewise "get rom-0 config.rom" transfers the configuration file on the Prestige to your computer and renames it "config.rom." See earlier in this chapter for more information on filename conventions.

Step 7. Enter "quit" to exit the ftp prompt.

The Prestige automatically restarts after a successful file upload.

21.4.4 FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 21-7 FTP Session Example of Firmware File Upload

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to *section 21.2.5* to read about configurations that disallow TFTP and FTP over WAN.

21.4.5 TFTP File Upload

The Prestige also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

Step 1. Use telnet from your computer to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.

Step 2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

Step 3. Enter the command "sys stdio 0" to disable the console timeout, so the TFTP transfer will not be interrupted. Enter "command sys stdio 5" to restore the five-minute console timeout (default) when the file transfer is complete.

Step 4. Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.

Step 5. Use the TFTP client (see the example below) to transfer files between the Prestige and the computer. The file name for the firmware is "ras".

Note that the telnet connection must be active and the Prestige in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "get" to transfer from the Prestige to the computer, "put" the other way around, and "binary" to set binary transfer mode.

21.4.6 TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the Prestige's IP address and "put" transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the Prestige).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

Chapter 22
System Maintenance

This chapter leads you through SMT menus 24.8 to 24.10.

22.1 Command Interpreter Mode Overview

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the zyxel.com web site for more detailed information on CI commands. Enter 8 from **Menu 24 — System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type "exit" to return to the SMT main menu when finished.

```
Menu 24 - System Maintenance

1.  System Status
2.  System Information and Console Port Speed
3.  Log and Trace
4.  Diagnostic
5.  Backup Configuration
6.  Restore Configuration
7.  Upload Firmware
8.  Command Interpreter Mode
9.  Call Control
10. Time and Date Setting
11. Remote Management

Enter Menu Selection Number:
```

Figure 22-1 Command Mode in Menu 24

```
Copyright (c) 1994 - 2003 ZyXEL Communications Corp.
p623me-t1> ?
Valid commands are:
sys             exit            ether           wan
etherdbg        usb             ip              bridge
p623me-t1>
```

Figure 22-2 Valid Commands

22.2 Call Control Support

Call Control Support is only applicable when **Encapsulation** is set to **PPPoE** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the Prestige within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 — System Maintenance — Call Control**, as shown in the next table.

```
                Menu 24.9 - System Maintenance - Call Control

                   1.  Budget Management



                          Enter Menu Selection Number:
```

Figure 22-3 Menu 24.9 System Maintenance : Call Control

22.2.1 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 — System Maintenance — Call Control** to bring up the following menu.

```
                        Menu 24.9.1 - Budget Management

  Remote Node        Connection Time/Total Budget      Elapsed Time/Total Period
1. MyISP                      No Budget                        No Budget
2.--------                       ---                              ---
3.--------                       ---                              ---
4.--------                       ---                              ---
5.--------                       ---                              ---
6.--------                       ---                              ---
7.--------                       ---                              ---
8.--------                       ---                              ---

                      Reset Node (0 to update screen):
```

Figure 22-4 Menu 24.9.1 Budget Management

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node when PPPoE encapsulation is selected.

Table 22-1 Menu 24.9.1 Budget Management

FIELD	DESCRIPTION	EXAMPLE
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)	1
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1.	5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed.
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.	0.5/1 means that 30 minutes out of the 1 hour time period has lapsed.
Enter "0" to update the screen or press [ESC] to return to the previous screen.		

22.3 Time and Date Setting

The Prestige keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your Prestige. Menu 24.10 allows you to update the time and date settings of your Prestige. The real time is then displayed in the Prestige error logs.

Select menu 24 in the main menu to open **Menu 24 System Maintenance**, as shown next.

```
                    Menu 24 - System Maintenance

                   1.  System Status
                   2.  System Information
                   3.  Log and Trace
                   4.  Diagnostic
                   5.  Backup Configuration
                   6.  Restore Configuration
                   7.  Upload Firmware
                   8.  Command Interpreter Mode
                   9.  Call Control
                   10. Time and Date Setting
                   11. Remote Management

                    Enter Menu Selection Number:
```

Figure 22-5 Menu 24 System Maintenance

Then enter 10 to go to **Menu 24.10 System Maintenance Time and Date Setting** to update the time and date settings of your Prestige as shown in the following screen.

```
          Menu 24.10 - System Maintenance - Time and Date Setting

     Use Time Server when Bootup= None
     Time Server Address= N/A

     Current Time:                          00 : 00 : 00
     New Time (hh:mm:ss):                   11 : 23 : 16

     Current Date:                          2000 - 01 - 01
     New Date (yyyy-mm-dd):                 2001 - 03 - 01

     Time Zone= GMT

     Daylight Saving= No
     Start Date (mm-dd):                              01 - 00
     End Date (mm_dd):                                01 - 00


               Press ENTER to Confirm or ESC to Cancel:
```

Figure 22-6 Menu 24.10 System Maintenance: Time and Date Setting

Table 22-2 Menu 24.10 System Maintenance: Time and Date Setting

FIELD	DESCRIPTION
Use Time Server when Bootup	Enter the time service protocol that your time server sends when you turn on the Prestige. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to **Time (RFC-868)**. **None**. The default, enter the time manually.
Time Server Address	Enter the IP address or domain name of your time server. Check with your ISP/network administrator if you are unsure of this information.
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you re-enter this menu.
New Date	Enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	If you use daylight savings time, then choose **Yes**.
Start Date	If using daylight savings time, enter the month and day that it starts on.
End Date	If using daylight savings time, enter the month and day that it ends on
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

22.3.1 Resetting the Time

The Prestige resets the time in three instances:

i. On leaving menu 24.10 after making changes.

ii. When the Prestige starts up, if there is a time server configured in menu 24.10.

iii. 24-hour intervals after starting.

Chapter 23
Remote Management

This chapter covers remote management (SMT menu 24.11).

23.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which Prestige interface (if any) from which computers.

23.2 Configuring Remote Management

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

Enter 11 from menu 24 to display **Menu 24.11 — Remote Management Control**.

23.2.1 Remote Management Setup

You may manage your Prestige from a remote location via:

the Internet (**WAN only**), the **LAN only**, **All** (LAN and WAN) or **Disable** (neither).

- WAN only (Internet)
- ALL (LAN and WAN)
- LAN only
- Disable (Neither)

If you enable remote management of a service, but have applied a filter to block the service, then you will not be able to remotely manage the service.

Enter 11, from menu 24, to display **Menu 24.11 — Remote Management Control** (shown next).

```
                Menu 24.11 - Remote Management Control

TELNET Server:
  Server Port = 23                  Server Access = LAN only
  Secured Client IP = 0.0.0.0

FTP Server:
  Server Port = 21                  Server Access = LAN only
  Secured Client IP = 0.0.0.0

Web Server:
  Server Port = 80                  Server Access = LAN only
  Secured Client IP = 0.0.0.0


             Press ENTER to Confirm or ESC to Cancel:
```

Figure 23-1 Menu 24.11 Remote Management Control

The following table describes the fields in this menu.

Table 23-1 Menu 24.11 Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
Telnet Server FTP Server Web Server	Each of these read-only labels denotes a service that you may use to remotely manage the Prestige.	
Server Port	This field shows the port number for the remote management service. You may change the port number for a service if needed, but you must use the same port number to use that service for remote management.	23
Server Access	Select the access interface (if any) by pressing the [SPACE BAR]. Choices are: **LAN only**, **WAN only**, **All** or **Disable**. The default is **LAN only**.	**LAN only**
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the Prestige. Enter an IP address to restrict access to a client with a matching IP address.	0.0.0.0
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.		

23.2.2 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.

2. You have disabled that service in menu 24.11.
3. The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
4. There is already another remote management session of the same type (Telnet, FTP or Web) running. You may only have one remote management session of the same type running at one time.
5. There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.

23.3 Remote Management and NAT

When NAT is enabled:

- Use the Prestige's WAN IP address when configuring from the WAN.
- Use the Prestige's LAN IP address when configuring from the LAN.

23.4 System Timeout

There is a system timeout of five minutes (300 seconds) for Telnet/web/FTP connections. Your Prestige will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

Chapter 24
IP Policy Routing

This chapter covers setting and applying policies used for IP routing.

24.1 IP Policy Routing Overview

Traditionally, routing is based on the destination address only and the IAD takes the shortest path to forward a packet. IP Routing Policy (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

24.2 Benefits of IP Policy Routing

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Quality of Service (QoS) – Organizations can differentiate traffic by setting the precedence or TOS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.

24.3 Routing Policy

Individual routing policies are used as part of the overall IPPR process. A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria includes the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, TOS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, for example, telnet, tend to have short packets, while bulk traffic, for example, file transfer, tends to have large packets.

The actions that can be taken include:

- routing the packet to a different gateway (and hence the outgoing interface).
- setting the TOS and precedence fields in the IP header.

IPPR follows the existing packet filtering facility of RAS in style and in implementation. The policies are divided into sets, where related policies are grouped together. A user defines the policies before applying them to an interface or a remote node, in the same fashion as the filters. There are 12 policy sets with six policies in each set.

24.4 IP Routing Policy Setup

Menu 25 shows all the policies defined.

```
                Menu 25 - IP Routing Policy Setup

Policy                                  Policy
Set #          Name                     Set #          Name
------  -----------------               ------  -----------------
  1     test                              7     _________________
  2     _________________                 8     _________________
  3     _________________                 9     _________________
  4     _________________                10     _________________
  5     _________________                11     _________________
  6     _________________                12     _________________


                Enter Policy Set Number to Configure= 0

                Edit Name= N/A

                Press ENTER to Confirm or ESC to Cancel:
```

Figure 24-1 Menu 25 IP Routing Policy Setup

To setup a routing policy, perform the following procedures:

Step 1. Type 25 in the main menu to open **Menu 25 – IP Routing Policy Setup.**

Step 2. Type the index of the policy set you want to configure to open **Menu 25.1 – IP Routing Policy Setup**.

Menu 25.1 shows the summary of a policy set, including the criteria and the action of a single policy, and whether a policy is active or not. Each policy contains two lines. The former part is the criteria of the incoming packet and the latter is the action. Between these two parts, separator "|" means the action is taken on criteria matched and separator "=" means the action is taken on criteria not matched.

```
                    Menu 25.1 - IP Routing Policy Setup

 # A                          Criteria/Action
 - - ------------------------------------------------------------------------------
 1 Y SA=1.1.1.1-1.1.1.1,DA=2.2.2.2-2.2.2.5
     SP=20-25,DP=20-25,P=6,T=NM,PR=0              |GW=192.168.1.1,T=MT,PR=0
 2 N ____________________________________________________________________________
     ____________________________________________________________________________
 3 N ____________________________________________________________________________
     ____________________________________________________________________________
 4 N ____________________________________________________________________________
     ____________________________________________________________________________
 5 N ____________________________________________________________________________
     ____________________________________________________________________________
 6 N ____________________________________________________________________________
     ____________________________________________________________________________

Enter Policy Rule Number (1-6) to Configure:
```

Figure 24-2 Menu 25.1 IP Routing Policy Setup

Table 24-1 Menu 25.1 IP Routing Policy Setup

ABBREVIATION		MEANING
Criterion	SA	Source IP Address
	SP	Source Port
	DA	Destination IP Address
	DP	Destination Port
	P	IP layer 4 protocol number (TCP=6, UDP=17…)
	T	Type of service of incoming packet
	PR	Precedence of incoming packet
Action	GW	Gateway IP address
	T	Outgoing Type of service
	P	Outgoing Precedence
Service	NM	Normal
	MD	Minimum Delay
	MT	Maximum Throughput
	MR	Maximum Reliability
	MC	Minimum Cost

Type a number from 1 to 6 to display **Menu 25.1.1 – IP Routing Policy** (see the next figure). This menu allows you to configure a policy rule.

```
                        Menu 25.1.1 - IP Routing Policy

          Policy Set Name= test
          Active= Yes
          Criteria:
            IP Protocol    = 6
            Type of Service= Normal           Packet length= 40
            Precedence     = 0                  Len Comp= N/A
            Source:
              addr start= 1.1.1.1             end= 1.1.1.1
              port start= 20                  end= 20
            Destination:
              addr start= 2.2.2.2             end= 2.2.2.2
              port start= 20                  end= 20
          Action= Matched
            Gateway addr   = 192.168.1.1      Log= No
            Type of Service= Max Thruput
            Precedence     = 0

                                Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 24-3 Menu 25.1.1 IP Routing Policy

The following table describes the fields in this menu.

Table 24-2 Menu 25.1.1 IP Routing Policy

FIELD	DESCRIPTION
Policy Set Name	This is the policy set name assigned in **Menu 25 – IP Routing Policy Setup**.
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate or No to deactivate the policy. Inactive policies are displayed with a minus sign "-" in SMT menu 25.
Criteria :	
IP Protocol	IP layer 4 protocol, for example, **UDP**, **TCP**, **ICMP**, etc.
Type of Service	Prioritize incoming network traffic by choosing from **Don't Care**, **Normal**, **Min Delay**, **Max Thruput, Min Cost** or **Max Reliable**.
Precedence	Precedence value of the incoming packet. Press [SPACE BAR] and then [ENTER] to select a value from **0** to **7** or **Don't Care**.
Packet Length	Type the length of incoming packets (in bytes). The operators in the **Len Comp** (next field) apply to packets of this length.

Table 24-2 Menu 25.1.1 IP Routing Policy

FIELD	DESCRIPTION
Len Comp	Press [SPACE BAR] and then [ENTER] to choose from **Equal**, **Not Equal**, **Less**, **Greater**, **Less or Equal** or **Greater or Equal**.
Source:	
addr start / end	Source IP address range from start to end.
port start / end	Source port number range from start to end; applicable only for TCP/UDP.
Destination:	
addr start / end	Destination IP address range from start to end.
port start / end	Destination port number range from start to end; applicable only for TCP/UDP.
Action	Specifies whether action should be taken on criteria **Matched** or **Not Matched**.
Gateway addr	Defines the outgoing gateway address. The gateway must be on the same subnet as the Prestige if it is on the LAN, otherwise, the gateway must be the IP address of a remote node. The default gateway is specified as 0.0.0.0.
Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing **No Change**, **Normal**, **Min Delay**, **Max Thruput**, **Max Reliable** or **Min Cost**.
Precedence	Set the new outgoing packet precedence value. Values are **0** to **7** or **No Change**.
Log	Press [SPACE BAR] and then [ENTER] to select **Yes** to make an entry in the system log when a policy is executed.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

24.5 Applying an IP Policy

This section shows you where to apply the IP policies after you design them.

24.5.1 Ethernet IP Policies

From **Menu 3 — Ethernet Setup**, type 2 to go to **Menu 3.2 — TCP/IP and DHCP Ethernet Setup**.

You can choose up to four IP policy sets (from 12) by typing their numbers separated by commas, for example, 2, 4, 7, 9.

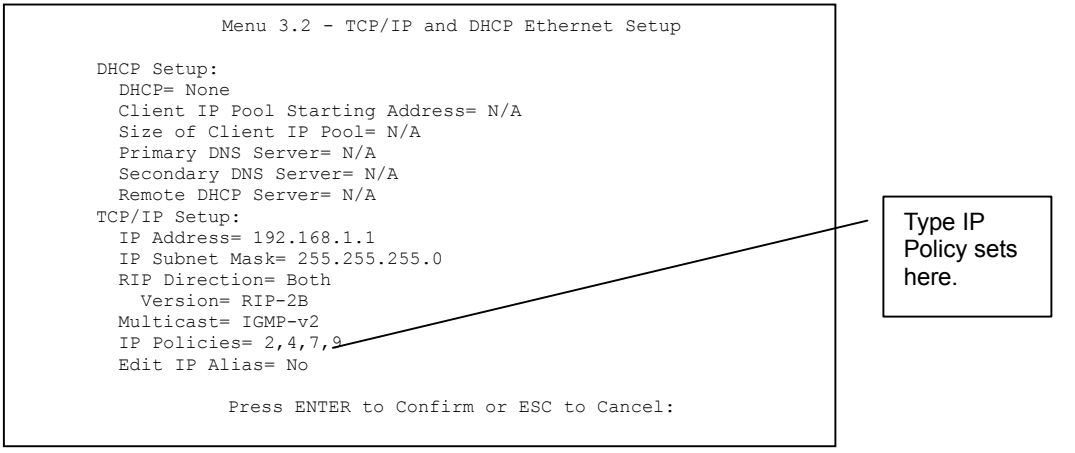

Menu 3.2 - TCP/IP and DHCP Ethernet Setup
DHCP Setup:
DHCP= None
Client IP Pool Starting Address= N/A
Size of Client IP Pool= N/A
Primary DNS Server= N/A
Secondary DNS Server= N/A
Remote DHCP Server= N/A
TCP/IP Setup:
IP Address= 192.168.1.1
IP Subnet Mask= 255.255.255.0
RIP Direction= Both
Version= RIP-2B
Multicast= IGMP-v2
IP Policies= 2,4,7,9
Edit IP Alias= No
Press ENTER to Confirm or ESC to Cancel:
Type IP Policy sets here.

Figure 24-4 Menu 3.2 TCP/IP and DHCP Ethernet Setup

Go to menu 11.3 (shown next) and type the number(s) of the IP Routing Policy set(s) as appropriate. You can cascade up to four policy sets by typing their numbers separated by commas.

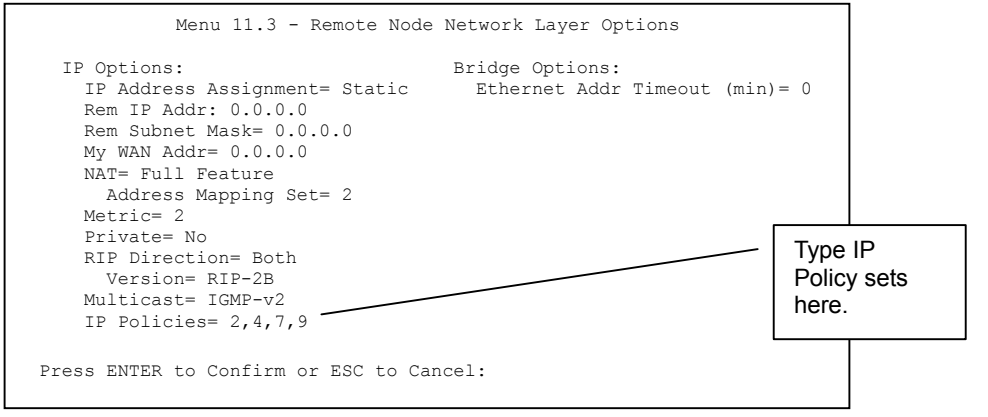


Figure 24-5 Menu 11.3 Remote Node Network Layer Options

24.6 IP Policy Routing Example

If a network has both Internet and remote node connections, you can route Web packets to the Internet using one policy and route FTP packets to a remote network using another policy. See the next figure.

Route 1 represents the default IP route and route 2 represents the configured IP route.

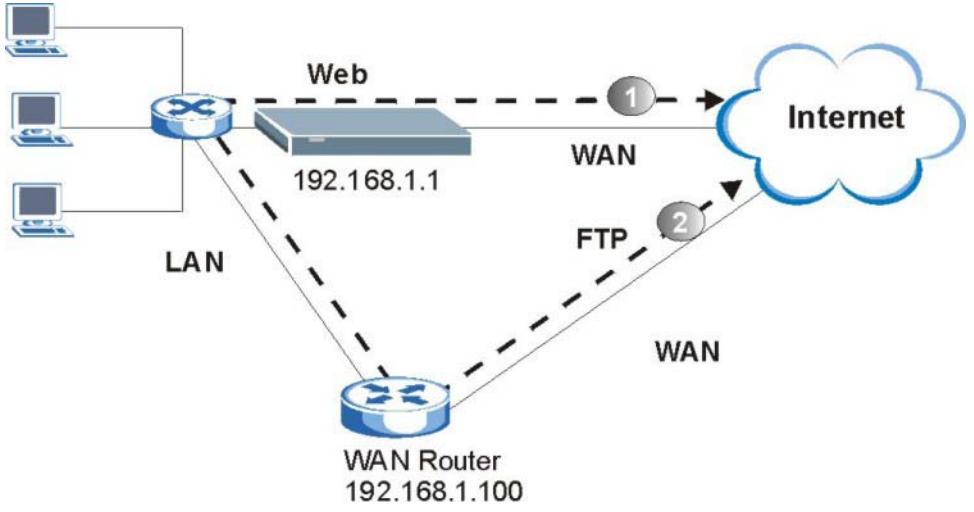


Figure 24-6 Example of IP Policy Routing

To force Web packets coming from clients with IP addresses of 192.168.1.33 to 192.168.1.64 to be routed to the Internet via the WAN port of the Prestige, follow the steps as shown next.

Step 1. Create a routing policy set in menu 25.

Step 2. Create a rule for this set in **Menu 25.1.1 — IP Routing Policy** as shown next.

```
                        Menu 25.1.1 - IP Routing Policy

          Policy Set Name= set1
          Active= Yes
          Criteria:
            IP Protocol    = 6
            Type of Service= Don't Care          Packet length= 10
            Precedence     = Don't Care            Len Comp= N/A
            Source:
                addr start= 192.168.1.33      end= 192.168.1.64
                port start= 0                 end= N/A
            Destination:
              addr start= 0.0.0.0             end= N/A
              port start= 80                  end= 80
          Action= Matched
            Gateway addr   = 192.168.1.1      Log= No
            Type of Service= No Change
            Precedence     = No Change

                    Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Figure 24-7 IP Routing Policy Example

Step 3. Check **Menu 25.1 — IP Routing Policy Setup** to see if the rule is added correctly.

Step 4. Create another policy set in menu 25.

Step 5. Create a rule in menu 25.1 for this set to route packets from any host (IP=0.0.0.0 means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

```
                                Menu 25.1.1 - IP Routing Policy

          Policy Set Name= set2

          Active= Yes
          Criteria:
            IP Protocol    = 6
            Type of Service= Don't Care            Packet length= 10
            Precedence     = Don't Care              Len Comp= N/A
            Source:
              addr start= 0.0.0.0                  end= N/A
              port start= 0                        end= N/A
            Destination:
              addr start= 0.0.0.0                  end= N/A
              port start= 20                       end= 21
          Action= Matched
            Gateway addr  =192.168.1.100           Log= No
            Type of Service= No Change
            Precedence     = No Change

                    Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Figure 24-8 IP Routing Policy Example

Step 6. Check **Menu 25.1 — IP Routing Policy Setup** to see if the rule is added correctly.

Step 7. Apply both policy sets in menu 3.2 as shown next.

```
                    Menu 3.2 - TCP/IP and DHCP Ethernet Setup

                      DHCP Setup
                        DHCP= Server
                        Client IP Pool Starting Address= 192.168.1.33
                        Size of Client IP Pool= 64
                        Primary DNS Server= 0.0.0.0
                        Secondary DNS Server= 0.0.0.0
                        Remote DHCP Server= N/A
                      TCP/IP Setup:
                        IP Address= 192.168.1.1
                        IP Subnet Mask= 255.255.255.0
                        RIP Direction= Both
                          Version= RIP-1
                        Multicast= None
                        IP Policies= 1,2
                        Edit IP Alias= No

                      Press ENTER to Confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

Figure 24-9 Applying IP Policies Example

Chapter 25
Call Scheduling

Call scheduling (applicable for PPPoE encapsulation only) allows you to dictate when a remote node should be called and for how long.

25.1 Call Scheduling Overview

The call scheduling feature allows the Prestige to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a video cassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 — Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 — Schedule Setup** as shown next.

```
                        Menu 26 - Schedule Setup

Schedule                                    Schedule
 Set #          Name                         Set #          Name
 ------   -----------------                  ------   -----------------
   1          AlwaysOn                         7
   2       _____________                       8       _____________
   3       _____________                       9       _____________
   4       _____________                      10       _____________
   5       _____________                      11       _____________
   6       _____________                      12       _____________

                   Enter Schedule Set Number to Configure=

                   Edit Name=

                   Press ENTER to Confirm or ESC to Cancel:
```

Figure 25-1 Menu 26 Schedule Setup

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 in are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the Prestige, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

To delete a schedule set, enter the set number and press [SPACE BAR] **and then** [ENTER] **(or delete) in the** Edit Name **field.**

To setup a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 — Schedule Set Setup** as shown next.

```
                        Menu 26.1 - Schedule Set Setup

                Active= Yes
                Start Date(yyyy-mm-dd) = 2000 - 01 - 01
                How Often= Once
                Once:
                  Date(yyyy-mm-dd)= 2000 - 01 - 01
                Weekdays:
                  Sunday= N/A
                  Monday= N/A
                  Tuesday= N/A
                  Wednesday= N/A
                  Thursday= N/A
                  Friday= N/A
                  Saturday= N/A
                Start Time (hh:mm)= 00 : 00
                Duration (hh:mm)= 00 : 00
                Action= Forced On

                          Press ENTER to Confirm or ESC to Cancel:
        Press Space Bar to Toggle
```

Figure 25-2 Menu 26.1 Schedule Set Setup

If a connection has been already established, your Prestige will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

Table 25-1 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the schedule set.	**Yes**
Start Date	Enter the start date when you wish the set to take effect in year - month-date format. Valid dates are from the present to 2036-February-5.	2000-01-01

Table 25-1 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION	EXAMPLE
How Often	Should this schedule set recur weekly or be used just once only? Press the [SPACE BAR] and then [ENTER] to select **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses.	**Once**
Once: Date	If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format.	2000-01-01
Weekday: Day	If you selected **Weekly** in the **How Often** field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select **Yes**, then press [ENTER].	**Yes** **No** **N/A**
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.	09:00
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.	08:00
Action	**Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line.	**Forced On**
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the **Main Menu** and then enter the target remote node index. Using [SPACE BAR], select **PPPoE** or **PPPoA** in the **Encapsulation** field and then press [ENTER] to make the schedule sets field available as shown next.

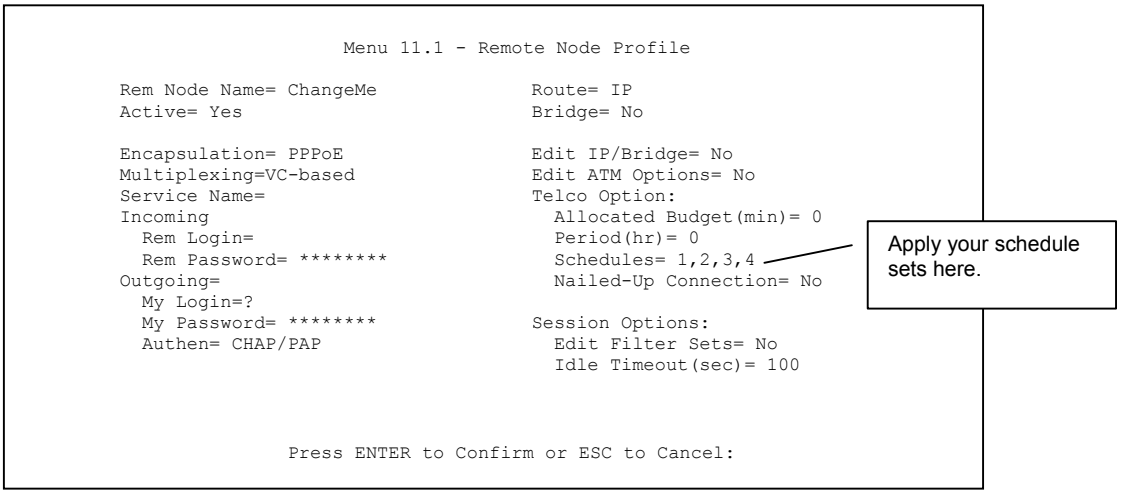


Figure 25-3 Applying Schedule Set(s) to a Remote Node (PPPoE)

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

Part VIII:

Appendices and Index

This part contains troubleshooting, additional background information and an index of key terms.

Appendix A Troubleshooting

This chapter covers potential problems and the corresponding remedies.

A.1 Using LEDs to Diagnose Problems

The LEDs are useful aides for finding possible problem causes.

A.1.1 Power LED

The **PWR** LED on the front panel does not light up.

Chart A-1 Troubleshooting Power LED

STEPS	CORRECTIVE ACTION
1	Make sure that the Prestige's power adaptor is connected to the Prestige and plugged in to an appropriate power source. Use only the supplied power adaptor.
2	Check that the Prestige and the power source are both turned on and the Prestige is receiving sufficient power.
3	Turn the Prestige off and on.
4	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

A.1.2 LAN LED

The **LAN** LED on the front panel does not light up.

Chart A-2 Troubleshooting LAN LED

STEPS	CORRECTIVE ACTION
1	Check the Ethernet cable connections between your Prestige and the computer or hub.
2	Check for faulty Ethernet cables.
3	Make sure your computer's Ethernet card is working properly.
4	If these steps fail to correct the problem, contact your local distributor for assistance.

A.1.3 DSL LED

The **DSL** LED on the front panel does not light up.

Chart A-3 Troubleshooting DSL LED

STEPS	CORRECTIVE ACTION
1	Check the telephone wire and connections between the Prestige DSL port and the wall jack.
2	Make sure that the telephone company has checked your phone line and set it up for DSL service.
3	Reset your ADSL line to reinitialize your link to the DSLAM. For details, refer to the *Maintenance* chapter (web configurator) or the System Information and Diagnosis chapter (SMT).
4	If these steps fail to correct the problem, contact your local distributor for assistance.

A.2 Telnet

I cannot telnet into the Prestige.

Chart A-4 Troubleshooting Telnet

STEPS	CORRECTIVE ACTION
1	Check the LAN port and the other Ethernet connections.
2	Make sure you are using the correct IP address of the Prestige. Check the IP address of the Prestige.
3	Ping the Prestige from your computer. If you cannot ping the Prestige, check the IP addresses of the Prestige and your computer. Make sure your computer is set to get a dynamic IP address; or if you want to use a static IP address on your computer, make sure that it is on the same subnet as the Prestige.
4	Make sure you entered the correct username and password. The default username is "admin" and the default password is "1234". If you have forgot your username or password, refer to *Section A.4*.
5	If these steps fail to correct the problem, contact the distributor.

A.3 Web Configurator

I cannot access the web configurator.

Chart A-5 Troubleshooting Web Configurator

STEPS	CORRECTIVE ACTION
1	Make sure you are using the correct IP address of the Prestige. Check the IP address of the Prestige.
2	Make sure that there is not an SMT console session running.
3	Your computer's and the Prestige's IP addresses must be on the same subnet for LAN access.
4	If you changed the Prestige's LAN IP address, then enter the new one as the URL.
5	Remove any filters in SMT menu 3.1 (LAN) or menu 11.5 (WAN) that block web service.

The web configurator does not display properly.

Chart A-6 Troubleshooting Internet Browser Display

STEPS	CORRECTIVE ACTION
1	Make sure you are using Internet Explorer 5.0 and later versions.
2	Delete the temporary web files and log in again. In Internet Explorer, click **Tools**, **Internet Options** and then click the **Delete Files ...** button. When a **Delete Files** window displays, select **Delete all offline content** and click **OK**. (Steps may vary depending on the version of your Internet browser.)

A.4 Login Username and Password

I forgot my login username and/or password.

Chart A-7 Troubleshooting Login Username and Password

STEPS	CORRECTIVE ACTION
1	If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This will erase all custom configurations and restore all of the factory defaults including the password.
2	Press the **RESET** button for five seconds, and then release it. When the **SYS** LED begins to blink, the defaults have been restored and the Prestige restarts.

Chart A-7 Troubleshooting Login Username and Password

STEPS	CORRECTIVE ACTION
3	The default username is "admin". The default password is "1234". The **Password** and **Username** fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing.
4	It is highly recommended to change the default username and password. Make sure you store the username and password in a save place.

A.5 LAN Interface

I cannot access the Prestige from the LAN or ping any computer on the LAN.

Chart A-8 Troubleshooting LAN Interface

STEPS	CORRECTIVE ACTION
1	Check the Ethernet LEDs on the front panel. A LAN LED should be on if the port is connected to a computer or hub. If the 10M/100M LEDs on the front panel are both off, refer to *Section A.1.2*.
2	Make sure that the IP address and the subnet mask of the Prestige and your computer(s) are on the same subnet.

A.6 WAN Interface

Initialization of the ADSL connection failed.

Chart A-9 Troubleshooting ADSL Connection

STEPS	CORRECTIVE ACTION
1	Check the cable connections between the ADSL port and the wall jack. The DSL LED on the front panel of the Prestige should be on.
2	Check that your VPI, VCI, type of encapsulation and type of multiplexing settings are the same as what you collected from your telephone company and ISP.
3	Restart the Prestige. If you still have problems, you may need to verify your VPI, VCI, type of encapsulation and type of multiplexing settings with the telephone company and ISP.

I cannot get a WAN IP address from the ISP.

Chart A-10 Troubleshooting WAN Interface

STEPS	CORRECTIVE ACTION
1	The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name.
2	The username and password apply to PPPoE encapsulation only. Make sure that you have entered the correct **Service Type**, **User Name** and **Password** (be sure to use the correct casing). Refer to the *WAN Setup* chapter (web configurator) or the *Internet Access* chapter (SMT).

A.7 Internet Access

I cannot access the Internet.

Chart A-11 Troubleshooting Internet Access

STEPS	CORRECTIVE ACTION
1	Make sure the Prestige is turned on and connected to the network.
2	If the DSL LED is off, refer to *Section A.1.3*.
3	Verify your WAN settings. Refer to the *WAN Setup* chapter (web configurator) or the *Internet Access* chapter (SMT).
4	Make sure you entered the correct user name and password.
5	(In Germany) Make sure you have a UR-2 line. Contact your local telephone company for more information.

Internet connection disconnects.

Chart A-12 Troubleshooting Internet Connection

STEPS	CORRECTIVE ACTION
1	Check the schedule rules. Refer to the *Call Scheduling* chapter (SMT).
2	If you use PPPoE encapsulation, check the idle time-out setting. Refer to the *WAN* chapter (web configurator) or the *Remote Node Configuration* chapter (SMT).
3	Contact your ISP.

A.8 Remote Node Connection

I cannot connect to a remote node or ISP.

Chart A-13 Troubleshooting Connecting to a Remote Node or ISP

STEPS	CORRECTIVE ACTION
1	Check menu 4 or WAN screen to verify that the username and password are entered properly.
2	In menu 11.1, verify your login name and password for the remote node.
3	If these steps fail, you may need to verify your login and password with your ISP.

Appendix B
IP Subnetting

IP Addressing

Routers "route" based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class "A" addresses have a 0 in the left most bit. In a class "A" address the first octet is the network number and the remaining three octets make up the host ID.
- Class "B" addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class "B" address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class "C" addresses begin (starting from the left) with 1 1 0. In a class "C" address the first three octets make up the network number and the last octet is the host ID.
- Class "D" addresses begin with 1 1 1 0. Class "D" addresses are used for multicasting. (There is also a class "E" address. It is reserved for future use.)

Chart B-1 Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

Host IDs of all zeros or all ones are not allowed.

Therefore:

- A class "C" network (8 host bits) can have 2^8 –2 or 254 hosts.
- A class "B" address (16 host bits) can have 2^{16} –2 or 65534 hosts.

A class "A" address (24 host bits) can have 2^{24} –2 hosts (approximately 16 million hosts).

Since the first octet of a class "A" IP address must contain a "0", the first octet of a class "A" address can have a value of 0 to 127.

Similarly the first octet of a class "B" must begin with "10", therefore the first octet of a class "B" address has a valid range of 128 to 191. The first octet of a class "C" address begins with "110", and therefore has a range of 192 to 223.

Chart B-2 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191
Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	224 to 239

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 bits; each bit of the mask corresponds to a bit of the IP address. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The "natural" masks for class A, B and C IP addresses are as follows.

Chart B-3 "Natural" Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence

of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class "C" address using both notations.

Chart B-4 Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

The first mask shown is the class "C" natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class "C" address 192.168.1.0 with subnet mask of 255.255.255.0.

	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class "C"). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The "borrowed" host ID bit can be either "0" or "1" thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

In the following charts, shaded/bolded last octet bit values indicate host ID bits "borrowed" to form network ID bits. The number of "borrowed" host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after "borrowing") determines the number of hosts you can have on each subnet.

Chart B-5 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**0**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Chart B-6 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**1**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is $2^7 - 2$ or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an

actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

Chart B-7 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Chart B-8 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Chart B-9 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Chart B-10 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

Chart B-11 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	223	254	255

The following table is a summary for class "C" subnet planning.

Chart B-12 Class C Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Subnetting With Class A and Class B Networks.

For class "A" and class "B" addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class "B" address has two host ID octets available for subnetting and a class "A" address has three host ID octets (see *Chart B-1*) available for subnetting.

The following table is a summary for class "B" subnet planning.

Chart B-13 Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126

Chart B-13 Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Appendix C
PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your PC to an ATM PVC (Permanent Virtual Circuit) which connects to a xDSL Access Concentrator where the PPP session terminates (see the next figure). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

Benefits of PPPoE

PPPoE offers the following benefits:

1. It provides you with a familiar dial-up networking (DUN) user interface.
2. It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.
3. It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the PCs use traditional dial-up networking.

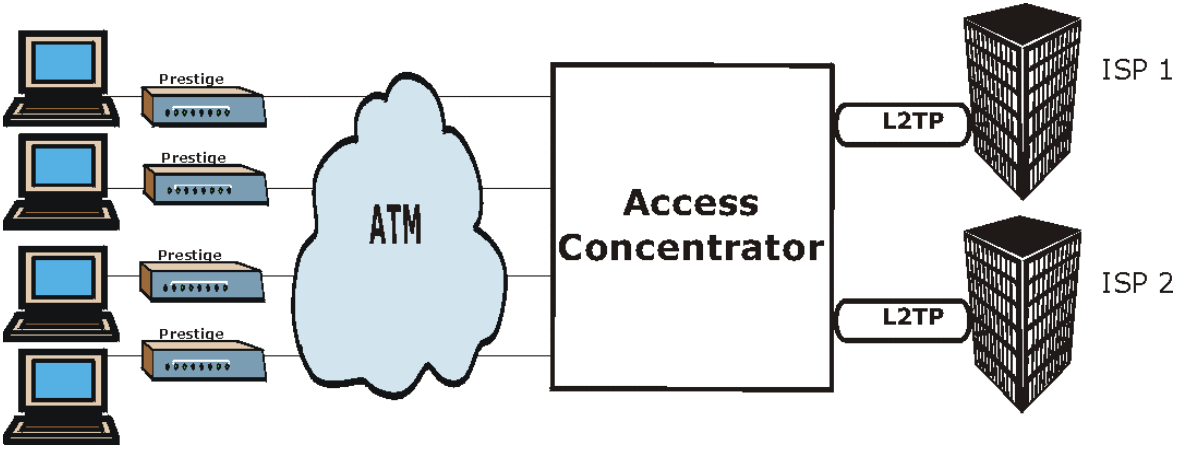


Diagram C-1 Single-PC per Router Hardware Configuration

How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the PC and the PC runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the PC and the ISP.

Prestige as a PPPoE Client

When using the Prestige as a PPPoE client, the PCs on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual PCs.

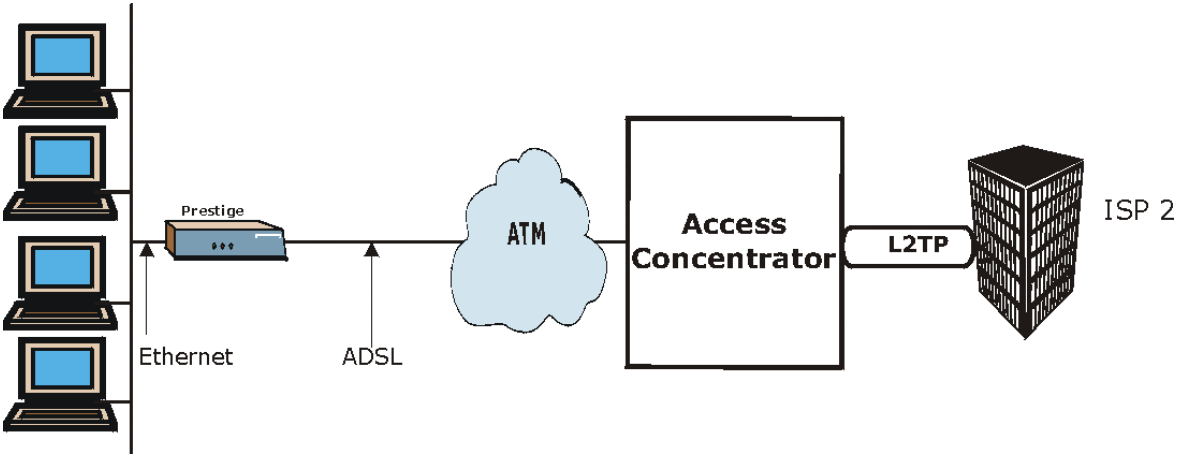


Diagram C-2 Prestige as a PPPoE Client

Appendix D
Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

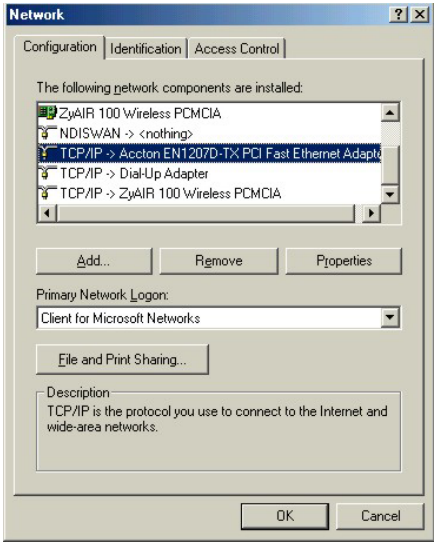
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Prestige's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

a. In the **Network** window, click **Add**.

b. Select **Adapter** and then click **Add**.

c. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

a. In the **Network** window, click **Add**.

b. Select **Protocol** and then click **Add**.

c. Select **Microsoft** from the list of **manufacturers**.

d. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

a. Click **Add**.

b. Select **Client** and then click **Add**.

c. Select **Microsoft** from the list of manufacturers.

d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

e. Restart your computer so the changes you made take effect.

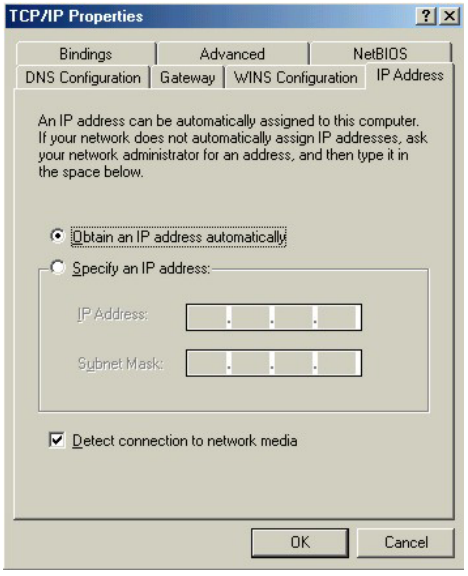
Configuring

1. In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**.

2. Click the **IP Address** tab.

   -If your IP address is dynamic, select **Obtain an IP address automatically**.

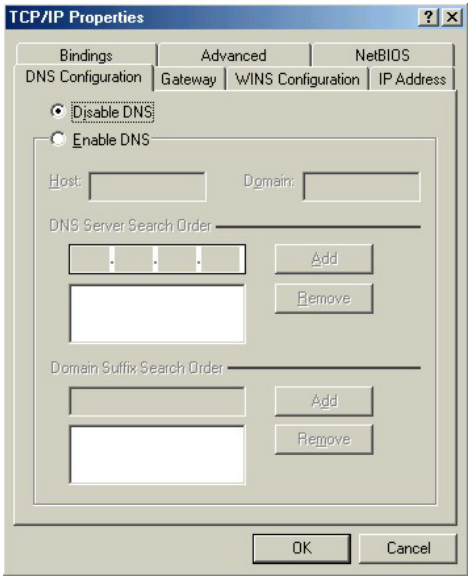
   -If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
Detect connection to network media
OK
Cancel

3. Click the **DNS Configuration** tab.

   -If you do not know your DNS information, select **Disable DNS**.

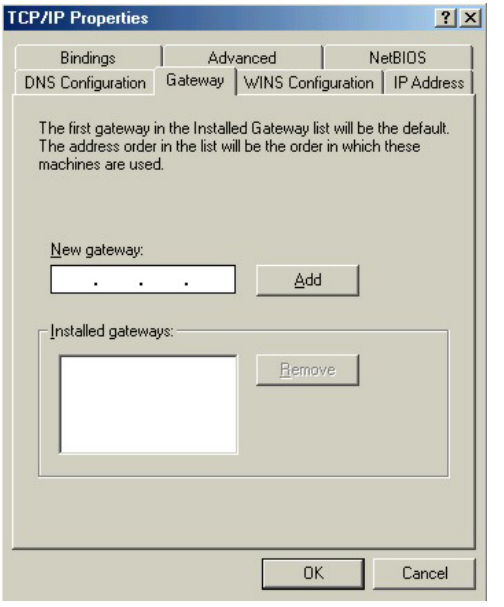
   -If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).



4. Click the **Gateway** tab.

   -If you do not know your gateway's IP address, remove previously installed gateways.

   -If you have a gateway IP address, type it in the **New gateway field** and click **Add**.



5. Click **OK** to save and close the **TCP/IP Properties** window.
6. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
7. Turn on your Prestige and restart your computer when prompted.

Verifying Settings

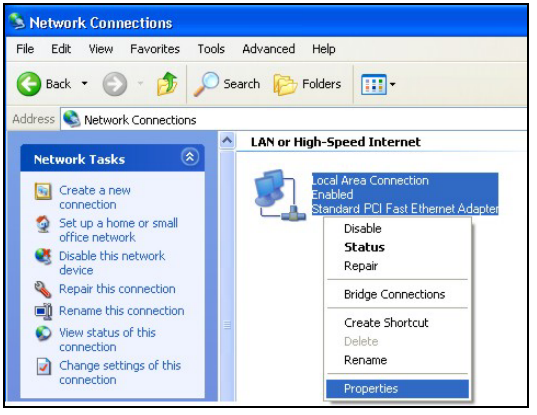
1. Click **Start** and then **Run**.
2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3. Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

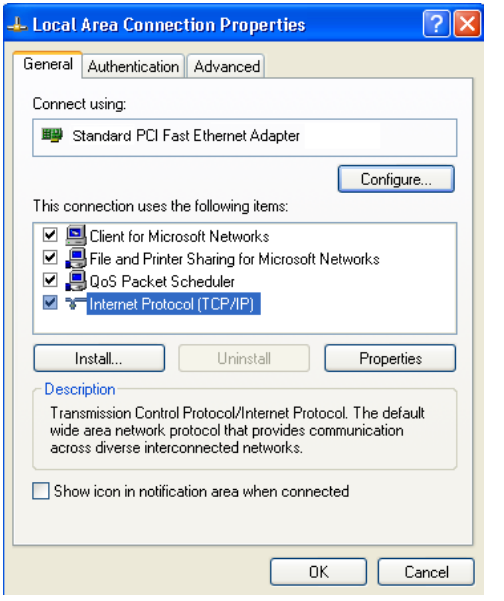
1. For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

2. For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

3. Right-click **Local Area Connection** and then click **Properties**.



4. Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

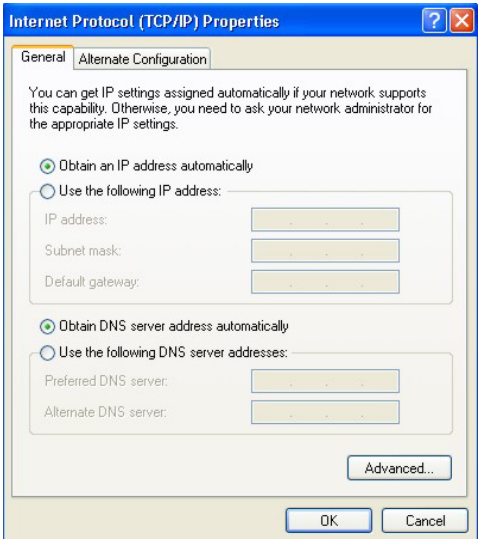


5. The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

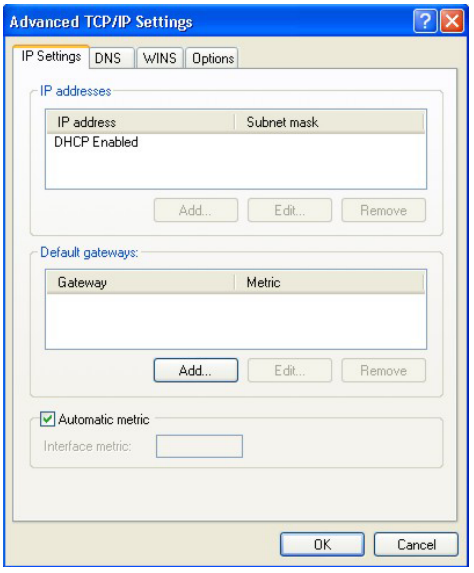
   -If you have a dynamic IP address click **Obtain an IP address automatically**.

   -If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.

   Click **Advanced**.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6. -If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Setting**s tab and click **OK**.



Do one or more of the following if you want to configure additional IP addresses:

-In the **IP Settings** tab, in IP addresses, click **Add**.

-In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.

-Repeat the above two steps for each IP address you want to add.

-Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

-In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.

-Click **Add**.

-Repeat the previous three steps for each default gateway you want to add.

-Click **OK** when finished.

7. In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

   -Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).

   -If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

   If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

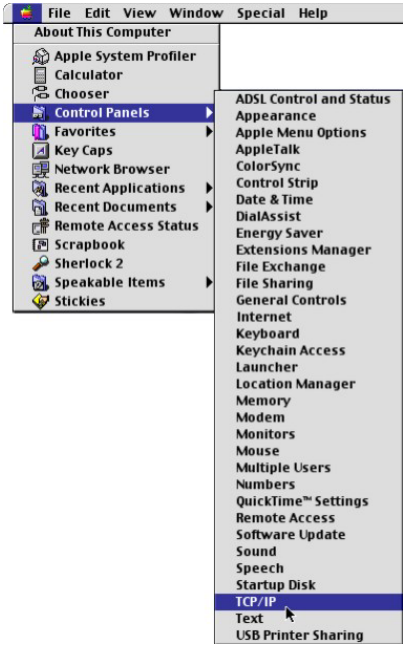
8. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
9. Click **OK** to close the **Local Area Connection Properties** window.
10. Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

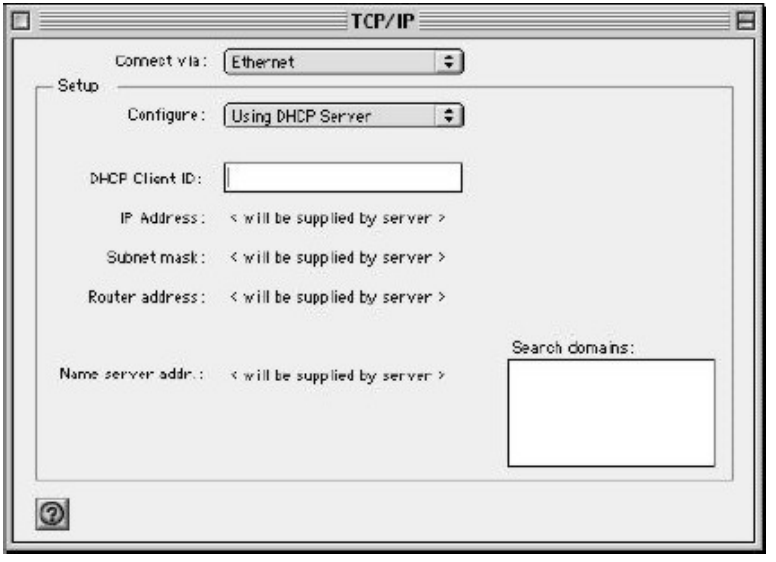
1. Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.
2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

1. Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.



2. Select **Ethernet built-in** from the **Connect via** list.



3. For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.
4. For statically assigned settings, do the following:

   -From the **Configure** box, select **Manually**.

   -Type your IP address in the **IP Address** box.

   -Type your subnet mask in the **Subnet mask** box.

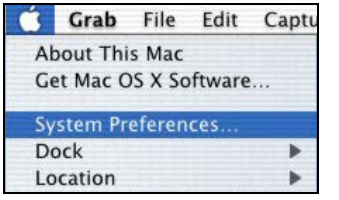
   -Type the IP address of your Prestige in the **Router address** box.
5. Close the **TCP/IP Control Panel**.
6. Click **Save** if prompted, to save changes to your configuration.
7. Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

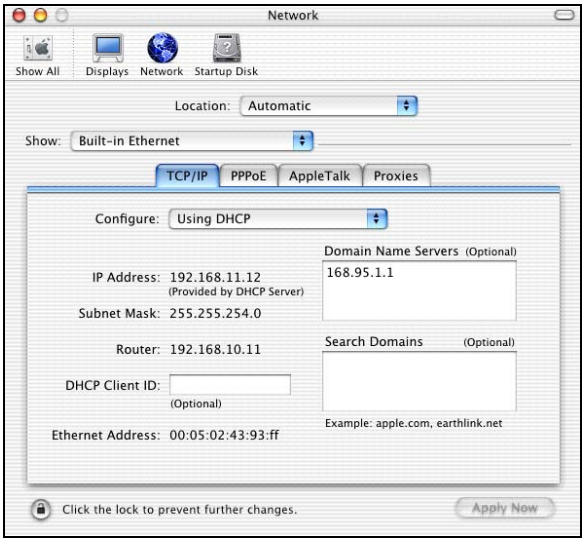
Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1. Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.



2. Click **Network** in the icon bar.
   - Select **Automatic** from the **Location** list.
   - Select **Built-in Ethernet** from the **Show** list.
   - Click the **TCP/IP** tab.



3. For dynamically assigned settings, select **Using DHCP** from the **Configure** list.
4. For statically assigned settings, do the following:
   -From the **Configure** box, select **Manually**.
   -Type your IP address in the **IP Address** box.
   -Type your subnet mask in the **Subnet mask** box.
   -Type the IP address of your Prestige in the **Router address** box.
5. Click **Apply Now** and close the window.
6. Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Appendix E
Virtual Circuit Topology

ATM is a connection-oriented technology, meaning that it sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

- Virtual Channel — Logical connections between ATM switches
- Virtual Path — A bundle of virtual channels
- Virtual Circuit — A series of virtual paths between circuit end points

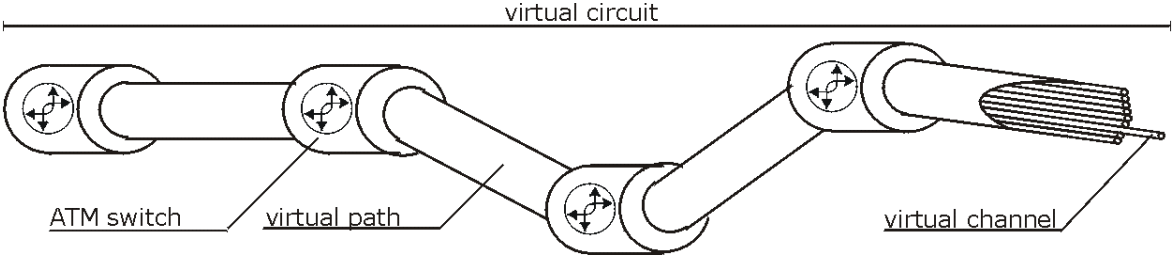


Diagram E-1 Virtual Circuit Topology

Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path.

The VPI and VCI identify a virtual path, that is, termination points between ATM switches. A series of virtual paths make up a virtual circuit.

Your service provider should supply you with VPI/VCI numbers.

Appendix F
Splitters and Microfilters

This appendix tells you how to install a POTS splitter or a telephone microfilter.

Connecting a POTS Splitter

When you use the Full Rate (G.dmt) ADSL standard, you can use a POTS (Plain Old Telephone Service) splitter to separate the telephone and ADSL signals. This allows simultaneous Internet access and telephone service on the same line. A splitter also eliminates the destructive interference conditions caused by telephone sets.

Install the POTS splitter at the point where the telephone line enters your residence, as shown in the following figure.

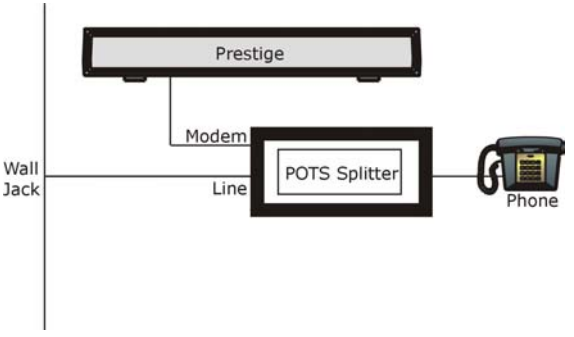


Diagram F-1 Connecting a POTS Splitter

Step 1. Connect the side labeled "Phone" to your telephone.

Step 2. Connect the side labeled "Modem" to your Prestige.

Step 3. Connect the side labeled "Line" to the telephone wall jack.

Telephone Microfilters

Telephone voice transmissions take place in the lower frequency range, 0 - 4KHz, while ADSL transmissions take place in the higher bandwidth range, above 4KHz. A microfilter acts as a low-pass filter, for your telephone, to ensure that ADSL transmissions do not interfere with your telephone voice transmissions. The use of a telephone microfilter is optional.

Step 1. Connect a phone cable from the wall jack to the single jack end of the Y- Connector.

Step 2. Connect a cable from the double jack end of the Y-Connector to the "wall side" of the microfilter.

Step 3. Connect another cable from the double jack end of the Y-Connector to the Prestige.

Step 4. Connect the "phone side" of the microfilter to your telephone as shown in the following figure.

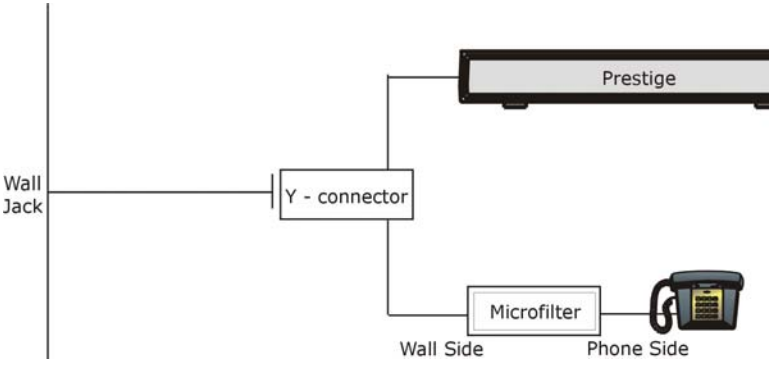


Diagram F-2 Connecting a Microfilter

Appendix G
Power Adaptor Specifications

NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	DV-1215A
Input Power	AC120Volts/60Hz/30W
Output Power	AC12Volts/1.25A
Power Consumption	11 W
Safety Standards	UL, CUL, CSA (UL 1310, CSA C22.2 No.223)
NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	AA-121A25
Input Power	AC120Volts/60Hz/19W
Output Power	AC 12Volts/ 1.25A
Power Consumption	11W
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223)
EUROPEAN PLUG STANDARDS	
AC Power Adapter Model	AA-121A3BN
Input Power	AC230Volts/50Hz/140mA
Output Power	AC12Volts/1.3A
Power Consumption	11W
Safety Standards	ITS-GS, CE (EN 60950)

Appendix H Index

A

Address Assignment 4-2
ADSL, what is it? xxix
Alternative Subnet Mask Notation B-3
AT command 20-1
Authentication 13-4, 13-5

B

Backup 20-2
Bridging 11-2
  Ether Address 15-4
  Ethernet 15-1
  Ethernet Addr Timeout 15-3
  Remote Node 15-1
  Static Route Setup 15-3
Budget Management 21-2, 21-3

C

Call Filtering 17-1
Call Filters
  Built-In 17-1
  User-Defined 17-1
Call Scheduling 24-1
  Maximum Number of Schedule Sets 24-1
  PPPoE 24-3
  Precedence 24-1
  Precedence Example ..... *See* precedence
CDR 19-7
CDR (Call Detail Record) 19-6
CHAP 13-4
Classes of IP Addresses B-1
Collision 19-3
Command Interpreter Mode 21-1
Community 18-2
Computer Name 10-1
Conditions that prevent TFTP and FTP from working over WAN 20-4
Configuration 3-7, 8-6
Copyright iii
Cost Of Transmission 13-7, 14-3
Country Code 19-4
CPU Load 19-3
Customer Support ix

D

Data Filtering 17-1
Device Filter rules 17-14
DHCP 3-7, 4-2, 6-1, 8-6, 19-4
Diagnostic Tools 19-1
DNS 11-3
Domain Name 4-2
Domain Name System 4-1
DSL (Digital Subscriber Line) xxix
DSLAM ..... *See* Digital Subscriber Line Access Multiplexer
Dynamic DNS 6-1, 10-2
DYNDNS Wildcard 6-1

E

Encapsulation 1-2, 3-1, 12-2, 13-2
  RFC 1483 3-2
Error Log 19-5
Error/Information Messages Sample 19-6
Ethernet Traffic 17-18

F

Factory LAN Defaults 4-2
FCC v

Filename Conventions 20-1
Filter 11-1
Applying Filters..... 17-17
Ethernet traffic..... 17-18
Ethernet Traffic 17-18
Filter log 19-7
Filter Rules 17-6
Filter Structure..... 17-4
Generic Filter Rule 17-12
Remote Node..... 13-9
Remote Node Filter 13-9
Remote Node Filters..... 17-18
Sample..... 17-16
SUA..... 17-14
TCP/IP Filter Rule..... 17-7
Filter log 19-8
Filter Rule..... 17-8
Filter Rule Process..... 17-3
Filter Rule Setup..... 17-7
Filter Rules Summary
Sample..... 17-17
Filter Set
Class 17-7
Filter Set Configuration 17-4
Filtering 17-1, 17-7
Filtering Process
Outgoing Packets..... 17-2
Firmware File
Maintenance 8-10
Forgot My Login Password A-3
Frame Relay..... 1-3
FTP 6-1, 22-2
Restrictions..... 22-2
FTP File Transfer..... 20-8
FTP Restrictions 6-1, 20-4
Full Rate F-1

G

Gateway..... 14-3
Gateway Node 15-4
General Setup 10-1

H

Hidden Menus 9-3
Hop Count 13-7, 14-3
Host 2-3
Host IDs..... B-1

I

IANA 3-4, 3-5
IGMP.....4-3
IGMP support.....13-8
Install UPnP.....7-3
Windows Me 7-3
Windows XP 7-4
Interactive Applications.....23-1
Internet access 12-1
Internet Access 1-1, 1-3, 11-2, 12-1, 12-2
Internet Access Setup A-5, 16-1
Internet Assigned Numbers Authority...*See* IANA
Introduction to DSL..... xxix
IP Address3-3, 4-3, 5-4, 8-6, 11-3, 14-3, 15-4, 17-9, 19-4, 19-9, 23-3
IP Address Assignment 3-4
PPPoA or PPPoE.....3-4
RFC 1483 3-4
IP Addressing B-1
IP Classes B-1
IP Filter.....17-11
Logic Flow 17-10
IP mask.....17-9
IP Packet.....17-12
IP Policies.....23-5
IP Policy Routing (IPPR) 1-2, 12-1
Applying an IP Policy 23-5
Ethernet IP Policies 23-5
Gateway 23-5
IP Pool Setup.....3-8
IP Protocol.....23-4
IP Routing Policy (IPPR) 23-1
Benefits 23-1
Cost Savings.....23-1

Criteria 23-1
Load Sharing 23-1
Setup 23-2
IP Routing Policy Setup 23-3
IP Static Route 14-1
IP Static Route Setup 14-2

L

LAN 19-3
LAN Setup 4-1
LAN TCP/IP 4-2
LLC-based Multiplexing 13-12
Log and Trace 19-6
Log Facility 19-7
Logging Option 17-9, 17-13
Login 13-4

M

MAC address 15-4
Main Menu 9-3
Management Information Base (MIB) 18-2
MBS ..... *See* Maximum Burst Size
Media Access Control 15-1
Message Logging 19-5
Metric 13-5, 13-7, 14-3
Multicast 4-3, 13-8
Multiplexing
LLC-based 3-2
VC-based 3-2
Multiplexing 1-2, 3-2, 12-3, 13-2
Multiprotocol Encapsulation 3-2
My WAN Address 13-7

N

NAT 3-3, 5-3, 17-14
Applying NAT in the SMT Menus 16-1
Configuring 16-3
Examples 16-3
NAT Traversal 7-1
Network Address Translation (NAT) 1-2, 16-1

P

Packet
Error 19-2
Received 19-3
Transmitted 19-3
Packet triggered 19-7
Packets 19-2
PAP 13-4
Password 2-3, *9-1*, 9-5, 13-4, 18-2
Ping 19-9
Point-to-Point xxix
policy-based routing 23-1
PPP Encapsulation 13-12
PPP log 19-7, 19-8
Precedence 23-1, 23-4
Private 13-7, 14-4
Protocol 17-8
Protocol Filter Rules 17-14

Q

Quality of Service 23-1
Quick Start Guide 2-1

R

RAS 19-4, 23-2
Rate
Receiving 19-2
Transmission 19-2
Read Me First xxvii
Related Documentation xxvii
Remote DHCP Server 11-3
Remote Management and NAT 6-2
Remote Management Limitations 6-1, 22-2
Remote Management Setup 22-1
Remote Node 13-1, 19-2
Remote Node Profile 13-3
Remote Node Setup 13-1, 13-2
Remote Node Index Number 19-2
Remote Node Traffic 17-19
Required fields 9-3

Restore Configuration 20-6
RIP .11-3, 13-7. *See* Routing Information Protocol
Routing Information Protocol 4-3
  Direction 4-3
  Version 4-3
Routing Policy 23-1

S

Sample IP Addresses 13-8
Schedule Sets
  Duration 24-2
SCR ..... *See* Sustain Cell Rate
Security 1-3
Server 16-3, 16-5, 21-5
Service vii
Service Type A-5
setup a schedule 24-2
Single User Account 5-1, 12-3
SMT Menu Overview 9-1
SNMP
  Community 18-3
  Configuration 18-2
  Get 18-2
  Manager 18-2
  MIBs 18-2
  Trap 18-2
  Trusted Host 18-3
SNMP (Simple Network Management Protocol)
  1-2
Source-Based Routing 23-1
Splitters F-1
Static Route Setup 14-1
Static Routing Topology 14-1
SUA 5-2
Subnet Mask 3-3, 4-3, 11-3, 13-7, 14-3, 19-4
Subnet Masks B-2
Subnetting B-2
Supporting Disk xxvii
Syntax Conventions xxvii
Syslog 19-6
Syslog IP Address 19-6
Syslog Server 19-6
System
  Console Port Speed 19-5
  Diagnostic 19-8
  Log and Trace 19-5
  Syslog and Accounting 19-6
  System Information 19-3
  System Status 19-1
System Information 19-3
System Information & Diagnosis 19-1
System Maintenance 19-1, 19-3, 20-2, 20-5, 20-11, 21-1, 21-2, 21-4, 21-5
System Management Terminal 9-3
System Status 19-2
System Timeout 6-2, 22-3

T

TCP/IP 6-2, 17-14, 19-9
Telephone Microfilters F-1
Telnet 6-2
Telnet Configuration 6-2
TFTP
  And FTP Over WAN} 22-2
  Restrictions 22-2
TFTP and FTP over WAN Will Not Work
  When… 20-4
TFTP and FTP Over WAN} 6-1
TFTP File Transfer 20-10
TFTP Restrictions 6-1, 20-4
Time and Date Setting 21-3, 21-4, 21-5
Time Zone 21-5
TOS (Type of Service) 23-1
Trace Records 19-5
Transmission Rates 1-1
Troubleshooting
  Internet Browser Display A-3
  Login Password A-3
  Power LED A-1, A-2
  Telnet A-2
  Web Configurator A-3
Type of Service 23-1, 23-3, 23-4, 23-5

U

Universal Plug and Play 7-1
Application 7-1
Security issues 7-1
Universal Plug and Play Forum 7-2
UNIX Syslog 19-5, 19-6
UNIX syslog parameters 19-6
Upload Firmware 20-8
UPnP ..... *See* Universal Plug and Play
User Name 6-2
Using LEDs To Diagnose Problems A-1

V

VPI & VCI 3-2

W

Web Configurator 2-1, 2-2
Wizard Setup 3-1

Z

ZyNOS 20-1, 20-2
ZyNOS F/W Version 20-1
ZyXEL Limited Warranty
Note vii